| | |
|---|---|
| Description of document: | **A History of U.S. Communications Security (Volumes I and II); the David G. Boak Lectures, National Security Agency, 1973** |
| Requested date: | 23-December-2007 |
| Released date: | 10-December-2008 |
| Posted date: | 24-December-2008 |
| Source of document: | National Security Agency<br>Attn: FOIA/PA Office (DJ4)<br>9800 Savage Road, Suite 6248<br>Ft. George G. Meade, MD 20755-6248<br>Phone: (301)-688-6527<br>Fax: (443)-479-3612 |
| Note: | The meat of the material left after redaction starts at (PDF) page 85. |

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

Serial: MDR-54498
10 December 2008

This responds to your request of 23 December 2007 to have A History of U.S. Communications Security (2 volumes) by David G. Boak, Fort George G. Meade, MD National Security Agency, 1973 reviewed for declassification. The material has been reviewed under the Mandatory Declassification Review (MDR) requirements of Executive Order (E.O.) 12958, as amended and is enclosed. We have determined that some of the information in the material requires protection.

Some portions deleted from the documents were found to be currently and properly classified in accordance with E.O. 12958, as amended. The information denied meets the criteria for classification as set forth in Section 1.4 subparagraphs (c) and (d) and remains classified SECRET and CONFIDENTIAL as provided in Section 1.2 of E.O. 12958, as amended.

Section 6.2 (c) of E.O. 12958, as amended, allows for the protection afforded to information under the provisions of law. Therefore, the names of NSA/CSS employees and information that would reveal NSA/CSS functions and activities have been protected in accordance with Section 6, Public Law 86-36 (50 U.S. Code 402 note).

Since your request for declassification has been denied you are hereby advised of this Agency's appeal procedures. Any person denied access to information may file an appeal to the NSA/CSS MDR Appeal Authority. The appeal must be postmarked no later than 60 calendar days after the date of the denial letter. The appeal shall be in writing addressed to the NSA/CSS MDR Appeal Authority

(DJP5), National Security Agency, 9800 Savage Road, STE 6884, Fort George G. Meade, MD 20755-6884. The appeal shall reference the initial denial of access and shall contain, in sufficient detail and particularity, the grounds upon which the requester believes the release of information is required. The NSA/CSS MDR Appeal Authority will endeavor to respond to the appeal within 60 working days after receipt of the appeal.

Sincerely,

Linda L. Huffman

LINDA L. HUFFMAN
Chief
Declassification Services

Encl:
a/s

VII - 26 - X

# A HISTORY OF U.S. COMMUNICATIONS SECURITY (U)
## (The David G. Boak Lectures)

### HANDLING INSTRUCTIONS

1. This publication consists of covers and numbered pages 1 to 101 inclusive. Verify presence of each page upon receipt.
2. Formal authorization for access to SECRET material is required for personnel to have access to this publication.
3. This publication will not be released outside government channels without approval of the Director, National Security Agency.
4. Extracts from this publication may be made for classroom or individual instruction purposes only. Such extracts will be classified SECRET NOFORN and accounted for locally until destroyed.
5. This publication will not be carried in aircraft for use therein.

NATIONAL SECURITY INFORMATION
Unauthorized Disclosure Subject to Criminal Sanctions

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755

Revised July 1973

Classified by Director, NSA, pursuant to NSA, Manual 123-2.
Exempt from General Declassification Schedule
of Executive Order 11652 Exempt Category 2.
Declassification date cannot be determined.

# INTRODUCTION

This publication consists of a series of lectures prepared and given to interns and other employees by Mr. David G. Boak in 1966. Mr. Boak is uniquely qualified to discuss the history of U.S. COMSEC because he has participated significantly in most aspects of its modern development over the past twenty years.

The purpose of these lectures was to present in an informal yet informative manner the fundamental concepts of Communications Security and to provide an insight into the strenghts and weaknesses of selected manual systems, electro-mechanical and electronic crypto-equipments.

## RECORD OF AMENDMENTS

| Identification of Amendment and No. (if any) | Date Entered | By Whom Entered (Signature; Rank or Rate; Name of Command) |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## RECORD OF PAGE CHECKS

| Date Checked | By Whom Checked (Signature; Rank or Rate; Name of Command) | Date Checked | By Whom Checked (Signature; Rank or Rate; Name of Command) |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

RECORD OF PAGE CHECKS

| Date Checked | By Whom Checked (Signature; Rank or Rate; Name of Command) | Date Checked | By Whom Checked (Signature; Rank or Rate; Name of Command) |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# TABLE OF CONTENTS

**FIRST LECTURE: The Need for Communications Security**

I will spend most of this first period belaboring some seemingly obvious points on the need for communications security; why we're in this business, and what our objectives really are. It *seems* obvious that we need to protect our communications because they consistently reveal our strengths, weaknesses, disposition, plans, and intentions and if the opposition intercepts them he can exploit that information by attacking our weak points, avoiding our strengths, countering our plans, and frustrating our intentions... something he can only do if he has advance knowledge of our situation. But there's more to it than that.

First, you'll note I said the opposition can do these things *if* he can intercept our communications. Let me first give you some facts about that supposition. You've all seen the security caveats asserting that "the enemy is listening", "the walls have ears", and the like. One of my irreverent friends, knowing where I work, insists on referring to me as "an electronic spy", and popular paperback literature is full of lurid stories about code-breakers and thieves in the night careening to Budapest on the Orient Express with stolen ciphers tattooed somewhere unmentionable. What is the actual situation? [redacted] their collection facilities include large land based sites, mobile platforms (air and sea), and satellite surveillance; and that they have an extensive covert collection operation. All in all, a truly formidable opponent. So the first "if" underlying our argument for the need for COMSEC (Communications Security) is more than a postulate—a deliberate, large, competent force has been identified whose mission is the exploitation of U.S. communications through their interception and analysis.

It is important to understand at the outset why the Soviet Union (as well as all other major countries) is willing to make an investment of this kind. Because, of course, they find it worthwhile. Sometimes, in the security business, you feel like a jackass having run around clutching defense secrets to your bosom only to find a detailed expose in *Missiles and Rockets* or the *Washington Post* or find it to be the subject of open conversations at a cocktail party or a coffee bar. There are, in fact, so many things that we cannot hide in an open society—at least in peace time—that you will sometimes encouter quite serious and thoughtful skepticism on the value or practicability of trying to hide anything ... particularly if the techniques you apply to hide information—like cryptography —entail money, loss of time, and constraints on action.

What then, is unique about communications intelligence? What does it provide that our mountains of literature and news do not similarily reveal? How can it match the output of a bevy of professional spies or in-place defectors buying or stealing actual documents, blueprints, plans? ("In-place defector"—a guy with a *bona fide* job in some place like the Department of Defense, the Department of State, this Agency, or in the contractual world who feeds intelligence to a foreign power.) It turns out that there *is* something special about communications intelligence, and it provides the justification for our own large expenditures as well as those of other countries: in a nutshell, its special value lies in the fact that this kind of intelligence is generally accurate, reliable, *authentic*, continuous, and most important of all, *timely*. The more deeply you become familiar with classified governmental operations, the more aware you will become of the superficiality and inaccuracy that is liable to characterize speculative journalism. After all, if we've done our job, we have reduced them to speculation—to the seizing of and elaboration on rumors, and to drawing conclusions based on very few hard facts. This is by no means intended as an indictment of the fourth estate—it is merely illustrative of why Soviet intelligence would rather have the contents of a message signed by a government official on a given subject or activity than a controlled news release or journalistic guess on the same subject. Similarly, the outputs of agents are liable to be fragmentary, sporadic, and *slow*; and there are risks entailed in the transmission of intelligence so acquired. [Conventional SIGINT (Signals Intelligence) activity, of course, entails no risk whatever.]

Let me track back again: I have said that there is a large and profitable intercept activity directed against us. This does not mean, however, that the Soviets or anybody else can intercept *all* our communications . . . that is, all of them at once; nor does it necessarily follow that all of them are *worth* intercepting. (The Army has a teletypewriter link to Arlington Cemetery through which they coordinate funeral arrangements and the like. Clearly a very low priority in our master plans for securing communications.) It does mean that this hostile SIGINT activity has to be selective, pick the communications entities carrying intelligence of most value or—and it's not necessarily the same thing—pick the targets most swiftly exploitable. Conversely, we in the COMSEC business are faced with the problem not simply of securing communications, but with the much more difficult problem of deciding which communications to secure, in what time frame, and with what degree of security. Our COMSEC resources are far from infinite; not only are there constraints on the money, people, and equipment we can apply but also—as you will see later on—there are some important limitations on our technology. We don't have that *secure* two-way wrist radio, for example.

In talking of our objectives, we can postulate an *ideal*—total security for all official U.S. Government communications; but given the limitations I have mentioned, our more realistic objectives are to develop and apply our COMSEC resources in such a way as to assure that we provide for our customers *a net advantage* vis-a-vis their opposite numbers. This means that we have to devise systems for particular applications that the opposition will find not necessarily *unbreakable* but too costly to attack because the attack will consume too much of his resources and *too much time*. Here, we have enormous variation—most of our big, modern electronic cryptosystems are designed to resist a full scale "maximum effort" analysis for many, many years; we are willing to invest a big expensive hunk of complicated hardware to assure such resistance when the underlying communications are of high intelligence value. At the other end of the spectrum we may be willing to supply a mere slip of paper designed only to provide security to a tactical communication for a few minutes or hours because the communication has no value beyond that time . . . an artillery spotter names a target; once the shell lands, hopefully on the coordinates specified, he couldn't care less about the resistance to cryptanalysis of the coded transmission he used to call for that strike.

Now, if the opposition brought to bear the full weight of their analytic resources they may be able to solve that code, predict that target, and warn the troops in question. But can they afford it? Collectively, the National Security Agency attempts to provide the commander with intelligence about the opposition (through SIGINT) while protecting his own communications against comparable exploitation—and thus provide the net advantage I spoke of. I'll state our practical objectives in COMSEC once more: not absolute security for all communications because this is too expensive and in some instances, may result in a net disadvantage; but sufficient security for each type of communications to make its exploitation uneconomical to the opposition and to make the recovery of intelligence cost more than its worth to him. Don't forget for a moment that some TOP SECRET messages may have close to infinite worth, though; and for these, we provide systems with resistance that you can talk of in terms of centuries of time and galaxies of energy to effect solution.

The reason I have spent this time on these general notions is the hope of providing you a perspective on the nature of the business we're in and some insights on why we make the kinds of choices we do among the many systems and techniques I'll be talking to you about during the rest of the week. I happened to start out in this business as a cryptanalyst and a designer of specialized manual systems not long after World War II. It seemed to me in those days that the job was a simplistic one—purely a matter of examining existing or proposed systems and, if you found anything wrong, fix it or throw the blighter out—period. In this enlightened spirit, I devised many a gloriously impractical system and was confused and dismayed when these magnificent products were sometimes rejected in favor of some clearly inferior—that is, *less secure* system merely because the alternative was simpler, or faster, or cheaper; or merely because it would *work*.

Those of you who are cryptanalysts will find yourselves in an environment that is necessarily cautious, conservative, and with security *per se* a truly paramount consideration. This, I assert, is *healthy* because you, a mere handful, are tasked with outthinking an opposing analytic force of perhaps 100 times your number who are just as dedicated to finding flaws in these systems as you must be to assuring none slipped by. But do not lose sight of the real world where your ultimate product must be used, and beware of security features so intricate, elaborate, complex, difficult, and expensive that our customers throw up their hands and keep on communicating in the clear—you have to judge not only the abstract probabilities of success of a given attack, but the likelihood that the opposition will be willing to commit his finite resources to it.

I hope you non-cryptanalysts smiling in our midst will recognize that we're playing with a two-edged sword—you are or ought to be in an environment where there is an enthusiasm for introducing to the field as many cryptosystems as possible at the least cost and with the fewest security constraints inhibiting their universal application. But don't kid yourselves: against the allegation that the COMSEC people of the National Security Agency—we're the villains—are quote pricing security out of the market unquote—is the fact that there is this monolithic opposing force that we can best delight by introducing systems which are not quite or not nearly as good as we think they are.

From this, we can conclude that, to carry out our job we have to do two things: first we have to provide systems which are cryptographically sound; and second, we have to insure that these systems can and will be used for the purpose intended.

If we fail in the first instance, we will have failed those customers who rely on our security judgments and put them in a disadvantageous position with respect to their opposition. But if we fail to get the systems used—no matter *how* secure they are—we are protecting nothing but our professional reputation.

Now that the general remarks about why we're in this business and what our objectives are are out of the way, we can turn to the meat of this course—my purpose, as much as anything, is to expose you to some concepts and teach you a new language, the vocabulary of the peculiar business you're in. To this end I will try to fix in your minds a number of rather basic notions or approaches that are applied in cryptography as well as a number of specific techniques as they have evolved over the past two decades.

There's a fair amount of literature—like the Friedman lectures—which is worth your time and which will trace the art of cryptography or ciphering back to Caesar or therabouts. I'll skip the first couple of millennia and such schemes as shaving a slave's head, writing a message on his shining pate, letting the hair grow back and dispatching him to Thermopylae or where have you. I'll also skip quite modern techniques of *secret writing*—secret inks, microphotography, and open letters with hidden meanings (called "innocent text" systems)—merely because their use is quantitatively negligible in the U.S. COMSEC scheme of things, and this Agency has practically nothing to do with them. What we will be addressing are the basic techniques and systems widely used in the protection of U.S. communications and which we are charged to evaluate, produce, or support.

All of our systems have one obvious objective: to provide a means for converting intelligible information into something unintelligible to an unauthorized recipient. We have discovered very few *basic* ways to do this efficiently. Some of the best ways of doing it have a fatal flaw; that is, that while it may be impossible for the hostile cryptanalyst to recover the underlying message because of the processing given it, neither can the intended recipient recover it because the process used could not be duplicated! On occasion there has been considerable wry amusement and chagrin on the part of some real professionals who have invented sophisticated encryption schemes only to find they were irreversible—with the result that not only the cryptanalyst was frustrated in recovering the plain text, so was the addressee. The inventor of a cryptosystem must not only find a means for rendering information unintelligible, he must use a process which is logical and reproducible at the receiving end. All of you know already that we use things called "keys" which absolutely determine the specific encryption process. It follows from what I have just said that we *always* produce at least two of them, one for the sender, one for the recipient. Through its application, and only through its application, the recipient is able to reverse, unscramble, or otherwise undo the encryption process.

The techniques that we have found useful so far amount to only two: first *substitution* of something meaningless for our meaningful text (our plain language); and second; *transposition*—keeping our original meaningful text, but jumbling the *positions* of our words or letters or digits so they no

EO 1.4.(c)

longer make sense. This latter technique is so fraught with security difficulties—it's nothing but fancy anagramming—that for all practical purposes you can toss it out of your lexicon of modern U.S. cryptography.

We are left with one very large family of systems in which the basic technique involves the substitution of one value for another. These range from systems whose security stems from a few letters, words, or digits memorized in somebody's head, through a variety of printed materials that permit encryption by use of paper and pencil, to the fancy electronic computer-like gadgets about which you have by now probably heard most. The first category of these systems we're going to talk about is *manual* systems and the first of these is *codes*. Professional cryptographers have been talking about codes, using them, attacking them, and solving them for many years. The traditional definition of them is: Code: "A substitution cryptosystem in which the plaintext elements are primarily words, phrases, or sentences, and the code equivalents (called "code groups") typically consist of letters or digits (or both) in otherwise meaningless combinations of identical length."—JUNE 71—*Basic Cryptologic Glossary*.

This definition provides a convenient way for differentiating a "code" from any other substitution system—all the other systems, which we call "ciphers", have a *fixed* relationship between the cipher value and its underlying meaning—each plaintext letter is always represented by one or two or some other specific number of cipher characters. Incidentally, we use "character" as a generic term to cover numbers or letters or digits or combinations of them. Let's look at a couple of codes:

1. The simplest kind, called a "one-part code", simply lists the plaintext meanings alphabetically (so that you can find them quickly) and some corresponding code groups (usually alphabetized also):

| | |
|---|---|
| BRIGADE . . . . . . . . . . . . . . . . . . . . . . . . . . . . | ABT |
| COORDINATE(S) . . . . . . . . . . . . . . . . . . . . . . . . | AXQ |
| DIRECT ARTILLERY FIRE AT____ . . . . . . . . . . . . . . . . . . | CDL |
| ENGAGE ENEMY AT . . . . . . . . . . . . . . . . . . . . | GGP |
| ------ . . . . . . . . . . . . . . . . . . . . . . . . | HLD |
| ------ . . . . . . . . . . . . . . . . . . . . . . . . | JMB |

There will usually be some numbers and perhaps an alphabet in such a code so that you can specify time and map coordinates and quantities and the like, and so that you can spell out words, especially place names, that could not be anticipated when the code was printed. Such a code has lots of appeal at very low echelons where only a very few stereotyped words, phrases, or directions are necessary to accomplish the mission. They are popular because they are simple, easy to use, and relatively fast. The security of such systems, however, is very, very low—after a handful of messages have been sent, the analyst can reconstruct the probable exact meanings of most of the code groups. We therefore take a dim view of them, and sanction their use only for very limited applications.

2. The kind of code we do use in very large quantities is more complicated, larger, and more secure. It is called a "two-part code": it is printed in two sections, one for encoding and the other for decoding:

| ENCODE | | DECODE | |
|---|---|---|---|
| BRIGADE . . . . . . . . . . . . . . . . | CDL | ABT . . . | ------ |
| COORDINATE(S) . . . . . . . . . . . . | AXQ | AXQ . . . | COORDINATE(S) |
| DIRECT ARTILLERY FIRE AT____ | JMB | CDL . . . | BRIGADE |
| ENGAGE ENEMY AT. . . . . . . . . | GGP | GGP . . . | ENGAGE ENEMY AT |
| ------ . . . . . . . . . . . . | HLD | HLD . . . | ------ |
| ------ . . . . . . . . . . . . | ABT | JMB . . . | DIRECT ARTILLERY FIRE AT____ |

The main thing that has been done here is to break up the alphabetical relationship between the plaintext meanings and the sequence of code groups associated with them—that is, the code groups are assigned in a truly random fashion, not in an orderly one. This complicates the cryptanalyst's job; but he can still get into the system rather quickly when the code is used repeatedly. As a result, a number of tricks are used to refine these codes and limit their vulnerability. The first trick is to provide more than one code group to represent the more commonly used words and phrases in the code vocabulary—we call these extra groups "variants" and in the larger codes in use today it is not uncommon to have as many as a half-dozen of these variants assigned to each of the high frequency (i.e., commonly used) plaintext values. Here's an excerpt from a code actually in use today showing some variants:

[redacted]

You probably know that "monoalphabetic substitution systems" were simple systems in which the same plaintext value was always represented by the same cipher or code value—repeats in the plain text would show up as repeated patterns in the cipher text, so lovely words like "RECONNAISSANCE" convert to, say,

```
RECONN AISSA NCE   . . . duck soup! it says here.
SDEGBB XMLLX BED
```

Well, with an ordinary code, that's exactly the problem. It is essentially a monoalphabetic system with a few variants thrown in, but with most repeated things in the transmitted code showing up as repeated items. This means, where we have to use codes (and later on, I'll show you why we have to in *huge* quantities), we have to do some things more fundamental than throwing in a few stumbling blocks like variants for the cryptanalyst. There are two techniques which are basic to our business and which we apply not only to codes but to almost all our keying materials. These are crucial to the secure management of our systems. These techniques are called *supersession* and *compartmentation*. They provide us a means for limiting the volume of traffic that will be encrypted in any given key or code; the effect of this limitation is to reduce the likelihood of successful cryptanalysis or of *physical loss* of that material; and further to reduce the scope of any loss that does occur.

SUPERSESSION is simply the replacement of a code or other keying material from time to time with new material. Most keys and codes are replaced each 24 hours; a few codes are replaced as frequently as each six hours; a few others remain effective for three days or more. We have these differing supersession rates because of the different ways in which the materials may be used. Holders of some systems may send only one message a day—everything else being equal, his system will have much greater resistance to cryptanalysis than that of a heavy volume user and his system will not quire replacement as often. The regular replacement rate of material each six hours or 24 hours or three days or what have you is called the "normal supersession rate" of the material in question. "Emergency supersession" is the term used when material is replaced prematurely because it may have been physically lost.

Once again, the purpose of periodic supersession of keying material and codes is to limit the amount of traffic encrypted in any one system and thus to reduce the likelihood of successful cryptanalysis or of physical loss; and to limit the effect of loss when it does occur. The resistance to cryptanalysis is effected by reducing the amount of material the cryptanalyst has to work on and by reducing the *time* he has available to him to get at *current* traffic.

COMPARTMENTATION is another means for achieving control over the amount of classified information entrusted to a specific cryptosystem. Rather than being geared to time, as in the case of supersession, it is geared to communications entities, with only those units that have to intercommunicate holding copies of any particular key or code. These communications entities in turn tend to be grouped by geography, service, and particular operational mission or specialty. Thus, the Army artillery unit based in the Pacific area would not be issued the same code being used by a similar unit in Europe—the vocabularies and procedures might be identical, but each would have unique code values so that loss of a code in the Pacific area would have no effect on the security of messages being sent in the Seventh Army in Europe, and vice versa. Of course some systems, particularly some machine systems, are designed specifically for intercommunication between two and only two holders—between point A and point B, and that's all. In such a case, the question of "compartmentation" doesn't really arise—the system is inherently limited to a compartment or "net" of two. But this is rarely the case with ordinary codes; and some of them must have a truly worldwide distribution. So our use of compartmentation is much more flexible and less arbitrary than our use of supersession; occasionally we will set some absolute upper limit on the number of holders permissible in a given system because cryptanalysis shows that when that number is exceeded, the ...ne to break the system is worth the hostile effort; but in general, it is the minimum needs, for intercommunication that govern the size (or, as we call it, the copy count) of a particular key list or code.

Now I have said that compartmentation and supersession are techniques basic to our whole business across the spectrum of systems we use. Their effect is to split our security systems into literally thousands of separate, frequently changing, *independent* entities. This means, of course, that the notion of "breaking *the* U.S. code" is sheer nonsense—the only event that could approach such catastrophic proportions for U.S. COMSEC would be covert (that is, undiscovered) penetration

[redacted]

The reason I've injected these concepts of compartmentation and supersession into the middle of this discussion of codes, although they have little to do with the structure of codes themselves, is that, despite our variants, and tricks to limit traffic volume, and controls over operational procedures, *codes as a class remain by far the weakest systems we use*; and these techniques of splitting them into separate entities and throwing them out as often as possible are essential to obtaining even the limited short-term security for which most of them are intended.

Having said, in effect, that codes as a class are not much good, let me point out that there are specialized paper and pencil systems which more or less conform to the definition of "code" but which are highly secure. Before I do this, let me return to the definition of code we started from, and suggest an alternative definition which more nearly pin-points how they *really* differ from other ...hniques of encryption. You remember we said the thing that makes a code unique is the fact that



EO 1.4.(c)

the code values can represent underlying values of different lengths—to recognize this is important to the cryptanalyst and that is the feature that stands out for him. But there is something even more basic and unique to a code: that is the fact that each code group—that QXB or what-have-you—stands for something that has *intrinsic meaning*, i.e., each underlying element of plain text is cognitive; it is usually a word or a phrase or a whole sentence. In every other system of encryption, this is not so; the individual cipher value stands only for an arbitrary symbol, meaningless in itself—like some binary digit or a letter of the alphabet. So I find, when examining a code, that QXB means "FIRE A GUN," or "REGROUP AT THE CROSSROADS," or "QUARTERBACK SNEAK," or what-have-you. In a *cipher* system, QXB might mean "X" or "L" or "001" or something else meaningless in itself. I've touched on this partly because the new cryptologic glossary has defined a code in terms of the meaning—or meaningfulness—of the underlying textual elements. I wouldn't push the distinction too far—it gets hazy when you are *spelling* with a code; get around it by admitting that, during the spelling process, you are in fact retaining a one-to-one relationship between the size of the underlying values and those being substituted for them—you are, for the moment, "enciphering" in the code.

*The "One-Time" Concept.*—I have said that at the heart of a code's insecurity is the fact that it is essentially a monoalphabetic process where the same code group always stands for the same underlying plaintext value. The way to lick this, of course, *is to devise a system where each code value is used once and only once.* Repeats don't show up because there aren't any, and we have effectively robbed the cryptanalyst of his "entering wedge" into the cryptosystem. Let's look at several such systems:

| | | | |
|---|---|---|---|
| ARTILLERY: | ABD | BRIGADE: | MJX |
| | QVM | | ZIY |
| | CXD | | RDF |
| | EVL | | QLW |
| | QSI | | |

.........
etc.

Well! This thing looks like nothing more than one of those ordinary codes we talked about, but with a set of variants assigned to each item of the vocabulary. Right. But suppose I make a rule that each time you use a variant, you check it off or cross it out, and must not use it again? By this simple expedient, I have given you a *one-time system*—a system which is for all practical purposes immune to cryptanalysis, perfectly secure? Sounds nice, and you might wonder why we have not adopted it for universal use. Well, let's look at some of the constraints inherent in this simple procedure:

Right now, if I have a very large vocabulary in a standard two-part code, it may run up to 32 pages or more. (The largest is 64 pages). If I have to insert say a half-dozen code values for every plaintext entry, my code book gets to be about 200 pages long, rather awkward to jam in the most voluminous of fatigue pockets, and a most difficult thing to thumb through—jumping back and forth, mind you—as you do your encoding or decoding process. So, limitation number one: we have to confine the technique to codes of quite small vocabularies.

Suppose my "compartment" (my net size) is 20 holders for this code. How does any given user know which values other holders in the net have used? He doesn't. He doesn't unless everybody listens to everybody else all the time, and that doesn't often happen. And this is really the killing limitation on most one-time systems of this kind. You wind up saying only *one* holder can send messages in the code, and all other copies are labelled "RECEIVE ONLY". We call this method of communications "Broadcast" and it has rather narrow applications. Alternatively, we can provide each of our 20 holders with a SEND code and 19 RECEIVE codes—but try to visualize some guy in an operational environment scrambling through 19 books to find the right one for a given incoming message; and look at the logistics to support such a system: it turns out that the number of books you need is the *square* of the number of holders you want to serve in this way—400 books for a 20-

holder net—10,000 for 100 holders! So limitation number two: the size of a net that you can practicably operate in this way is very small: preferably just two stations.

Let's turn now to another kind of one-time code; one that we call a "pro forma" system. "Pro forma" means that the basic framework, form or format of every message text is identical or nearly so; the same kind of information, message after message, is to be presented in the same order, and only specific values, *like numbers*, change with each message.

O 1.4

Now we're beginning to get something more manageable: We still have the constraint of needing a small net size or, alternatively, a larger net but with only one or a few senders of information. But it's a dandy where the form of the messages themselves permit this terrible inflexibility. We use a few of them, but machines are the things we're moving towards to meet most of the requirements of this type.

EO 1.4.(c)

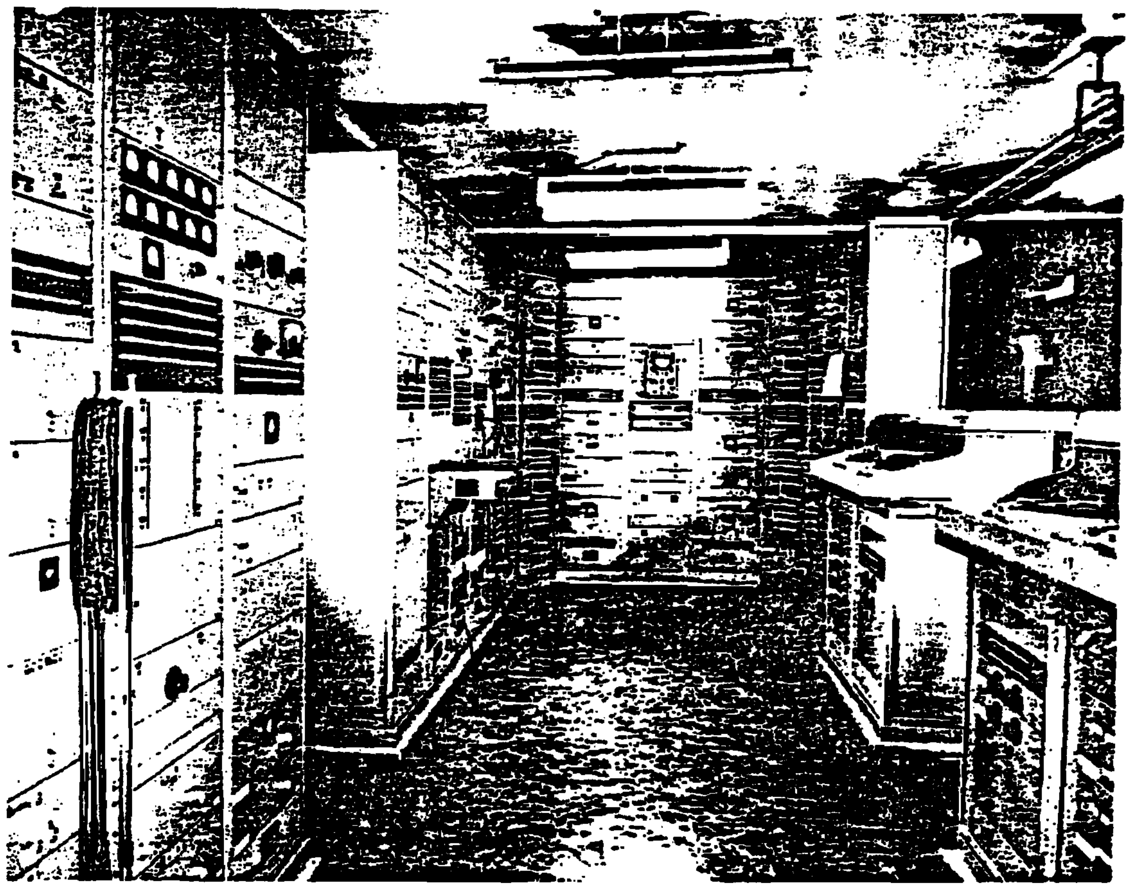
In comparing this one-time system and the last one I showed you, I think you'll begin to see a number of characteristics emerge for these specialized codes: first off, they are relatively secure: I say relatively, because there is more to communications security than resistance to cryptanalysis—and while these systems meet that first test—cryptanalysis—admirably, from the *transmission security* point of view, they're pretty bad; but we'll be talking about that on another day. Secondly: they are inflexible, rigidly confined with respect to the variety of intelligence they can convey. Thirdly: they are built for *speed*; they are by far the fastest means of communicating securely without a machine. Finally, they are extremely specialized, narrow in their application, and limited in the size of communications network they can serve efficiently. Being specialized, by the way, and *tailored* to particular needs, they fly in the face of efforts to *standardize* our materials—a very necessary movement in a business where we have to make hundreds of codes, distribute them all er the world, replace most of them daily and, as a result, wind up with a total copy count numbering, at the moment, about 5 million each year.

The business of standardizing on the one hand, for the sake of economy, simplicity, and manageability and of uniquely tailoring systems for maximum efficiency in some particular application, is one of the many conflicting or contradictory themes in our business; just as maximum security may conflict with speed or something else.

## SEVENTH LECTURE: Ciphony Equipment and Other Specialized Systems

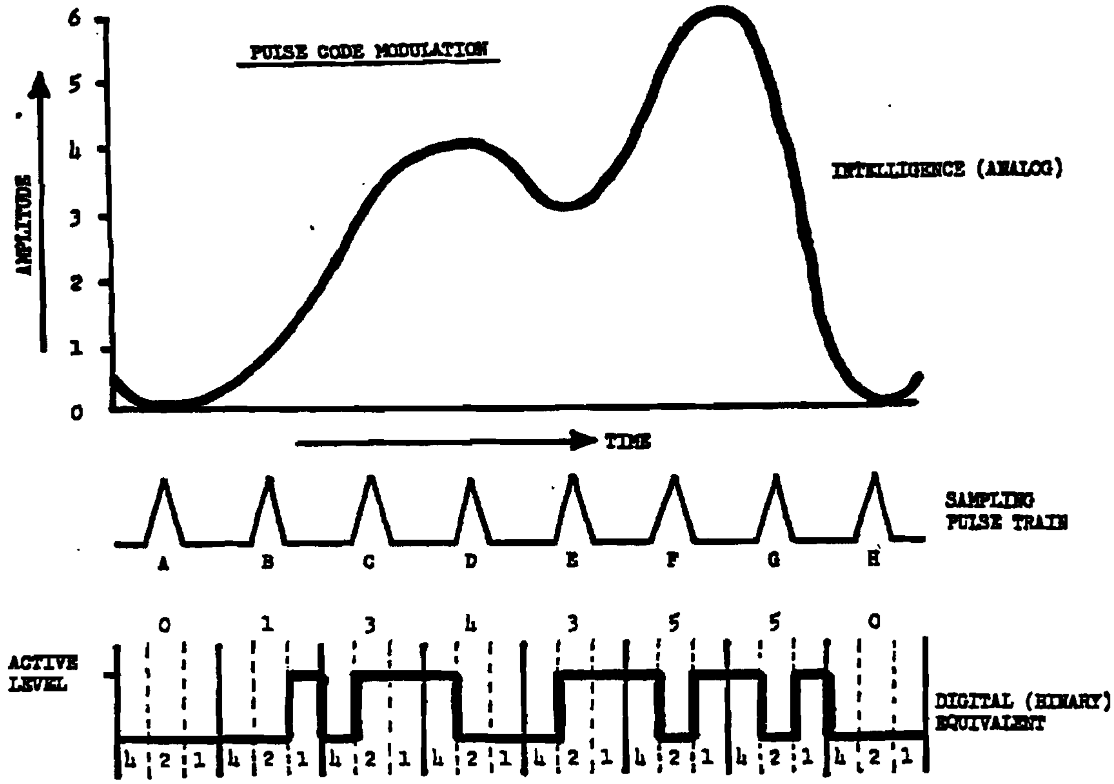
*Ciphony Equipment.*—You have already had a preview of some of the problems of voice encryption in the discussion of the KO-6. Since by far the greatest weakness in U.S. COMSEC today stems from the fact that almost all of our voice communications are sent in the clear, the business of finding economical secure ways to secure voice transmissions remains a burning issue and is consuming a good part of our current COMSEC R&D effort.

We have to go back to World War II for a look at our first voice encryption equipment:



This looks like a whole communications center or laboratory or something; but it's all one cipher machine. It was called SIGSALLY. If you counted the air-conditioners that had to go with it, it weighed something like 55 *tons*. It was used over the transatlantic cable for communication between Washington and London. It used vacuum tubes by the thousands, and had a primitive vocoder. It was hardly the answer to the dream of universal ciphony, and was dismantled soon after the war ended.

The next ciphony system to come along was called the AFSAY-816. It was designed to operate over microwave links—actually, just one link—between the Naval Security Station and Arlington Hall. Since there was plenty of bandwidth to play with (50 KHz), there were no constraints on the number of digits that could be used to convert speech into digital form. The technique used was called Pulse Code Modulation (PCM): conceptually, it involves sampling the amplitude (size) of an intelligence signal, such as one's voice, at fixed intervals of time determined by a high frequency pulse train, then transmitting the values thus obtained in some sort of binary or baudot code. The following illustration portrays these relationships:




The AFSAY-816 used a primitive vacuum tube key generator with bank after bank of shift registers . . . and, for the first time, we were able to put out more key than we could use. So we used it to provide for encryption of several channels of speech simultaneously. Speech quality was good, reliability was spotty, and security, especially in its last years was marginal since it was in about that time frame that we began to be able to postulate practical high-speed computer techniques as a cryptanalytical tool. We hastened to replace the equipment with one called the KY-11. The KY-11 was the first relatively modern key generator of the breed I described in the KW-26. [redacted]

EO 1.4.(c)

At any rate, we lived on borrowed time with the AFSAY-816 and on the hope that, because its transmitted signal was fast, complex, and directional, hostile interception and recording would be impracticable.

Don't think for a minute that the same rationale isn't used today for unsecured circuits that happen to use sophisticated transmission techniques. A favorite ploy of the manufacturers of forward tropospheric and ionospheric scatter transmission systems, for example, is to advertise them as inherently secure because of their directivity and because they are beamed over the horizon and theoretically bounce down in only one place. However, because of atmospheric anomalies; it is impossible to predict with certainty what the state of the ionosphere will be at any particular moment. It is because of these anomalies that the reflection of the transmitted signal from the ionosphere is subject to considerable variation and, consequently, subject to interception at an unintended location. As a matter of fact, there was a "permanently" anomalous situation over parts of Southeast Asia that caused VHF communications to double their expected range.

The general attitude of this Agency is that *no* deliberate transmission is free from the possibility of hostile interception. The thought is that there is really a contradiction in terms of the notion of an uninterceptible transmission: for, if there were such, the *intended* recipient, your own distant receiver, could not pick it up.

Despite all of this, it *is* clear that some transmissions are considerably more difficult and costly to intercept than others and some of them carrying information of low intelligence value may not be worth that cost to the potential hostile interceptor. These factors have a lot to do with the *priorities* we establish for providing cryptosystems to various kinds of communications entities.

But, in the case of voice, which is our subject, it has not been any rationale of non-interceptibility which has slowed us down, it is the set of terrifically difficult technical barriers in the way of getting such equipment in light, cheap, efficient, secure form, either for strategic high-level links, as in the case of all the ciphony equipments I've mentioned so far, or for tactical circuits that we will, in due course, cover.

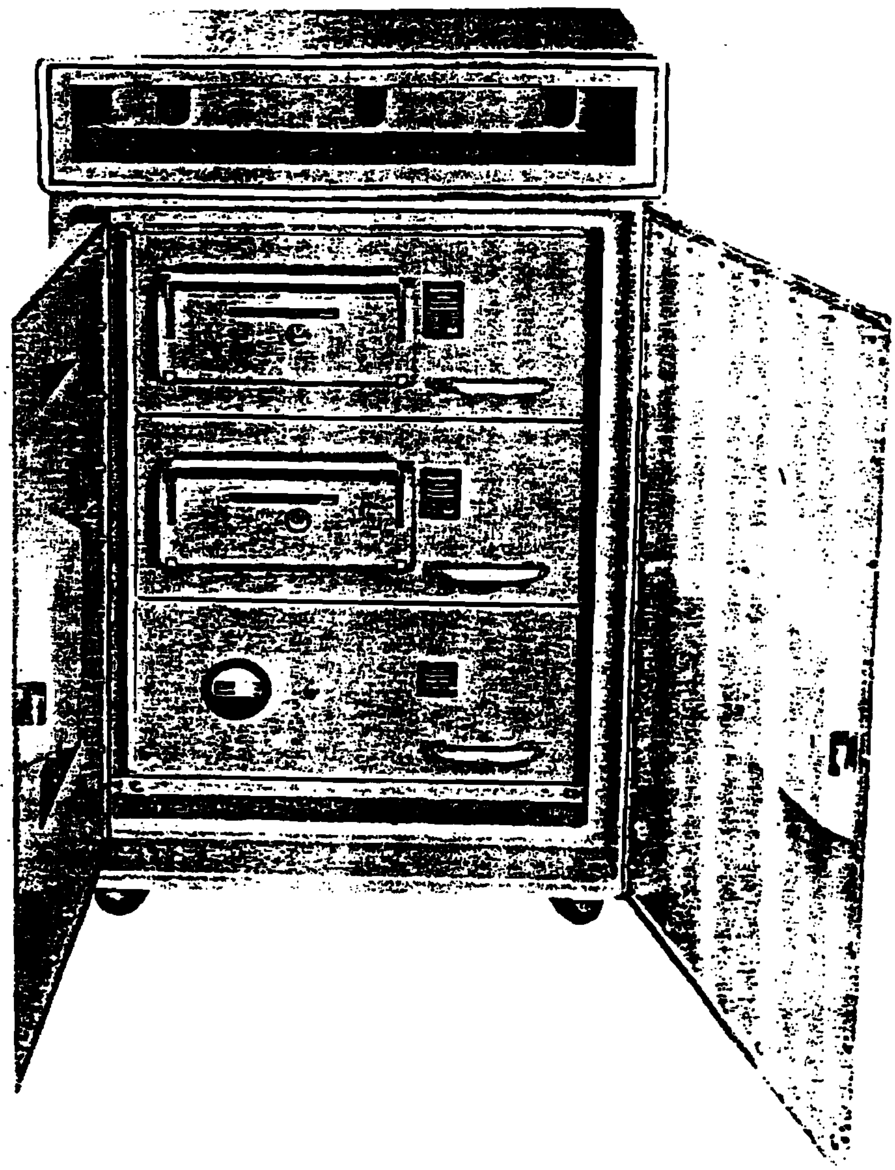
Still, with the advent of the KY-11, it appeared that we had at least one part of the ciphony problem relatively well in hand: that was for fixed-plant, short-range operations where plenty of bandwidth was available for transmission. These fixed-plant, wide-band equipments—all of them—not only could provide secure good quality voice, but had enough room to permit the encryption of several channels of voice with the same key generator. But just as in the case of teletypewriter security devices, there was a need to move ciphony equipment out of the cryptocenter and nearer to the environment where the actual user could have more ready access. In the case of the teletypewriter encryption systems, you will recall, the move was into the communications center where all the ancillary devices and communications terminal equipment and punched message tapes and message forms were readily available. In the case of ciphony, the real user was the individual who picks up the handset and talks—not some professional cryptographer or communicator—but people like you and me and generals and admirals and presidents. So the next need we faced was to provide an equipment which could be remote from both cryptocenter and communications center, and used right in the offices where the actual business of government and strategic military affairs is conducted. This called for machinery that was smaller and packaged differently than any of the ciphony equipment we have talked about thus far. SIGSALLY you remember, weighed 55 tons; the next system weighed a lot less but still needed 6 bays of equipment. The KY-11 was smaller still, amounting to a couple of racks of equipment configured for communications center use. None of them were at all suitable for installation in somebody's office.

The resultant product was called the TSEC/KY-1. The most striking feature it had, in contrast to its predecessor ciphony devices, was that it was neatly packaged in a single cabinet about two-thirds as tall and somewhat fatter than an ordinary safe. Because it was built not to be in a cryptocenter or a classified communications center where there are guards and controls on access to prevent theft of equipment and their supporting materials, this KY-1 cabinet was in fact a three-combination safe that contained the whole key generator, the power supply, the digitalizing voice preparation components—everything except the handset which sits on top.

So, for the first time since World War II with the SIGNIN, we found ourselves building physical protective measures into the equipment itself. The safe is not a particularly good one—hardly any are—but it is adequate to prevent really easy access to the classified components and keying data contained inside. Microwave links or special wire lines were used to transmit its 50 KHz cipher text. [redacted] and it had the capacity to link up to 50 holders through some kind of switchboard in a common key. The first network was used here in Washington and served key officials of government—the President, the Secretary of Defense, the Secretary of State, the Director, Central Intelligence Agency, and some others. We soon found that the equipment needed to be installed not only in key government offices, but in the private residences of key officials as well, so that they could consult securely in times of crisis night or day. I think the first such residence was EO 1.4.(c)

President Eisenhower's Gettysburg address: later such equipments were used in the homes of a number of other officials.

The KY-1 had some limitations, as almost all first tries at a new requirement seem to: it was essentially a push-to-talk system which annoys most users and makes it impossible to interrupt conversations. Eventually, the cryptanalysts discovered some new possible attacks that lowered our confidence in its security and so the KY-1 was retired in early 1967. This KY-3 is the follow-on equipment to the KY-1. It provides a duplex (no push-to-talk) capability and some security and operational refinements.

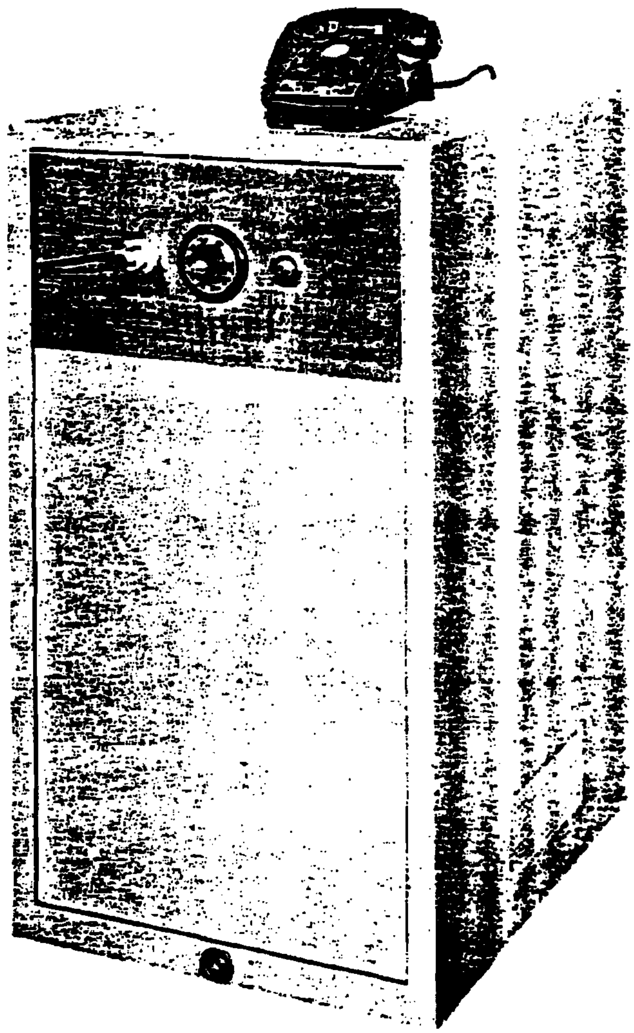


This is perhaps as good as a place as any to go off on another of the tangents that seem to characterize these lectures. As we have been following the evolution of U.S. cryptography, I have talked quite casually of new equipments coming into our inventory and old ones fading away. In retrospect, the demise of the obsolescent, inefficient, and insecure systems seems natural, easy, inevitable, and relatively painless. But the fact of the matter is that it is usually quite difficult to get the users to relinquish any equipment once it is solidly entrenched in their inventories—especially if it works well, as in the case of the KY-1; but even if it doesn't, as in the case of the KW-9. The reluctance to junk old systems stems from a number of causes, I think. First of all, they represent a large investment; secondly, the users have developed a supporting logistic base for the systems, have trained personnel to operate and maintain it—they've *used* it. Finally, the introduction of a new system is a slow and difficult business requiring new budgetary and procurement action, new training, the establishment of a new logistics base, and—increasingly these days—a costly installation job to match the new system to the facility and communications system in which it is to be used. Because of these problems, our "equipment retirement program" is a halting one, and only when there are very grave *security* shortcomings can we actually *demand* that a system be retired on some specific date. Well, back to ciphony systems.

With all these developments, we are still talking about equipment that weighs several hundred pounds, is quite expensive, and which is limited to specialized and costly communications links. Except in the case of the KO-6, these links are relatively short range.

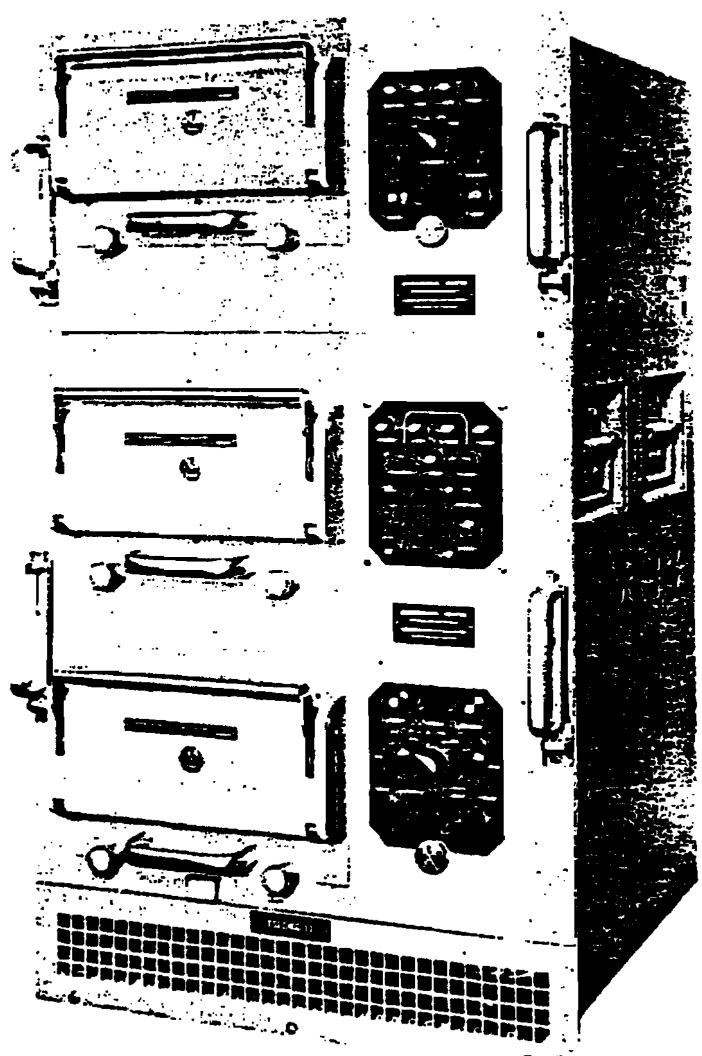
So, at the same time these wide-band fixed-plant equipments are being developed, we were working on something better than the KO-6 to satisfy long-range, narrow-band communications requirements, something that could, hopefully, be used on ordinary telephone lines or on HF radio circuits overseas. (Ma Bell's telephone system, you understand, has a bandwidth of only 3 KHz—and still has a few quick and dirty WW II links in the mid-west with only a 1500 hertz bandwidth. This situation, as I have said, sharply limits the number of digits we can use to describe speech to be encrypted on such circuits with a consequent loss of quality of intelligibility.)

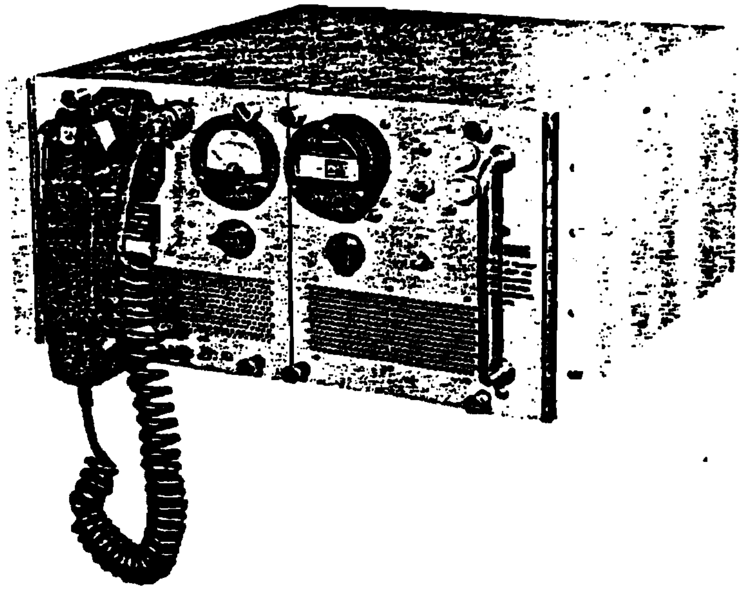
The equipment which evolved is called the KY-9.



The KY-9 used a vocoder as did its narrow-band predecessors, but a more sophisticated one than had been developed thus far. It was the first of the vocoders to use transistors instead of vacuum tubes, so that the equipment could be reduced to a single cabinet. But transistors were in their infancy; and the ones that went into the KY-9 were hand-made and expensive. Again the equipment was packaged into a safe so that it could be located in an office-type environment. Well, we were getting there: we could use an ordinary telephone line with the KY-9, but the speech still sounds artificial and strained because of that vocoder, and . . . you . . . must . . . speak . . . very . . . slowly . . . and . . . distinctly and you must still push to talk. And besides all that, this bear initially cost on the order of $40,000 per terminal which put it strictly in the luxury category. About 260 KY-9's are in use for high-level, long-haul voice security communications. The majority of the KY-9 subscribers are now being provided this secure capability through use of the Automatic Secure Voice Communications (AUTOSEVOCOM) system; however, it is anticipated that the equipment will remain in use at least through FY-74. Beyond FY-74, the equipment may be declared excess and stored for contingency purposes.

The best and newest long-haul voice equipment uses none other than our multi-purpose friend, the KG-13. Nobody came along with a nice vocoding speech digitalizer to hook into this key generator, and there's really not much call to process speech this way unless you're going to encrypt it, so we wound up—*again*—having to build some of the ancillary equipment ourselves. This equipment is called the HY-2—remember, the H stands for *ancillary*, the Y for *speech encryption*. So the combination referred to as the KG-13/HY-2 is the system we are now counting on to serve the long-haul voice requirement.





Again, a vocoder was used, and this sounds the best yet, although it still can't match the voice quality that wide-band systems have. This package is not in a safe, and is not suitable for office installation, but it seems to satisfy most of the other long-haul requirements well and does so fairly cheaply for the first time.

Before we talk about tactical voice security equipment, there is a subject related to the big fixed-plant voice equipments we ought to talk about. That's the subject of "approved" circuits. Way back with the KO–6, we were having difficulty getting officials to leave their offices and walk to a cryptocenter to use a secure phone. The solution lay in carrying the system or at least the telephone handset (which is all he really needs or cares about) to him. This involved running a wire line from an office to the cryptocenter or secure communications center. The difficulty with this solution is twofold: in the first place there was and is a long-standing Executive Order of the President governing the way classified information may be handled, transmitted, and stored; and in the case of TOP SECRET information, this order forbids electrical transmission *except in encrypted form*. Of course, the informations in the clear, not encrypted, until it reaches the cryptomachine, and this meant that any time one placed that handset remote from the machine, the user, by "law" had to be restricted to conversations no higher than SECRET. This is difficult to legislate and control, and reduces the usefulness of the whole system. The second difficulty in this situation stems from the security reasoning lying behind that Executive Order. The reasoning was, and is, that it is extremely difficult to assure that no one will tap any subscriber line such as this, if it is not confined to a very carefully controlled area like a cryptocenter or classified communications center. It means that if you are to use these subscriber lines in some government installation, the whole building or complex of buildings must be extremely well guarded, access carefully controlled, or personnel cleared or escorted all the time. Controls such as we have here are simply not feasible in a facility such as the Pentagon or on a typical military post; yet it is in just such environments that these protected wirelines may be needed.

Some special rules govern communications used to support SIGINT operations, and these rules have been interpreted to permit TOP SECRET traffic such as we use on the grey phone system here—provided certain physical and electronic safeguards are enforced. The JCS applied the same sort of criteria in staffing an action which permitted TOP SECRET information to be passed in the clear over wire lines when certain rigid criteria are met. Until this action went through, we were unable to make full use of the ciphony capability we now have in systems such as the KG–13/HY–2, and subscribers were held to SECRET unless they were essentially co-located with the crypto-equipment itself.

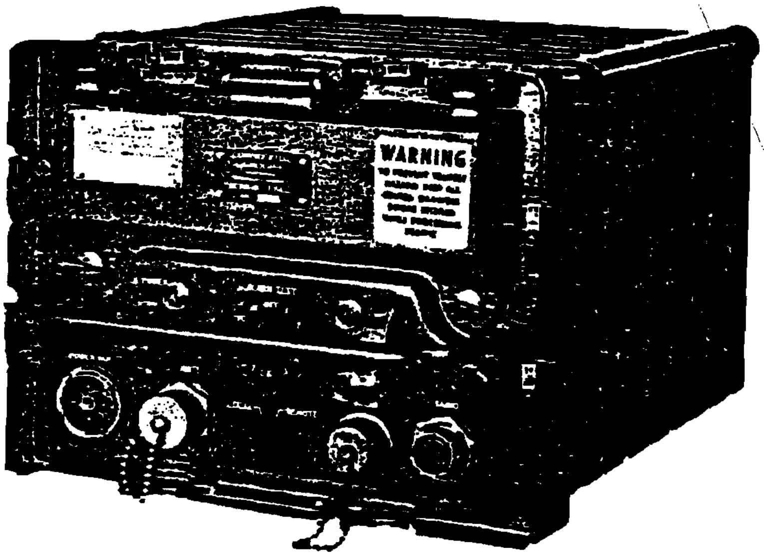
*Tactical Ciphony.*—MC's for tactical ciphony equipment—be they broad-band, narrow-band, or somewhere in between—have existed since before this Agency was created. But the difficulties were terrific. To have tactical usage on field telephones and radio telephones and military vehicles and, especially, in aircraft, the equipment had to be truly light, small, and rugged; and had to be compatible with a large variety of tactical communications systems most of which are not compatible among themselves. In the case of aircraft requirements, there's an old saying that the Air Force will reject any system unless it has no weight, occupies no space, is free, and adds lift to aircraft. We were about ready to believe this in the late fifties when we had gotten a tactical ciphony device, the KY-8, down to about 2/3 of a cubic foot, and it was still not accepted, mainly because it took up too much room. The ironic part of this sad story is that the cryptologic portion of the hardware uses only a modest amount of space: its power supplies and the digitalizers for speech that use up the room. The Air Force did give that small equipment, the KY-8, a good try in high performance aircraft like F-100's: it worked fairly well, but sometimes reduced the effective range of their radios about 5%, a degradation of their basic communications capability they simply could not afford. Besides, the problem of lack of space proved very real and they had to rip out one of their fire-control radars to make room for the test equipment.

Then the Army decided it could use the KY-8, mounting it in jeeps and other wheeled vehicles where space was not so critical as in aircraft. We had attempted to make a ground tactical ciphony equipment for Army, called the KY-4, but it didn't pan out; and the Army had independently tried to develop a tactical voice device that was equally unsuccessful. So Army bought a batch of KY-8's and they and the Marines became the principal users, even though it was really originally designed for aircraft.

There's another point about the KY-8. I've made it sound as if over-choosy users have been the only cause for its slowness in coming and limited use. That's not quite the case. There were some security problems—the compromising emanation business again—that slowed down our production for some time: we finally got going full blast on this equipment by cancelling out most of the delaying features in the contract associated with the radiation problem, accepting this possible security weakness as a calculated risk, and placing some restrictions on where the equipment could be used to minimize that risk.

Today we have a family of compatible, tactical speech security equipments known as NESTOR—the KY-8/28/38. The KY-8 is used in vehicular and afloat applications; the KY-28 is the airborne version; and the KY-38 is the portable or man-pack model. There are currently about 27,000 NESTOR equipments in the U.S. inventory. No further procurement of NESTOR equipments is planned because the VINSON equipment is intended to satisfy future requirements for wide-band tactical voice security.

EO 1.4.(c)




[redacted]

[redacted]

From the operational point of view, the effect of a system such as this is that any receiver can pick up a transmission in mid-stream just as KW-37 receivers can, but without the elaborate clocks and high-speed catch-up mechanisms. [redacted]

We have now covered the major equipments and principles in use today. The big systems are:

| | |
|---|---|
| For Literal Traffic: | The KL-7/47 |
| For Teletypewriter Traffic: | The KW-26, KW-37, KW-7 |
| For Ciphony: | The KY-3, KY-8, KY-9 (KG-13/HY-2 |
| For Multi-purpose: | The KG-3/KG-13 |

[redacted]

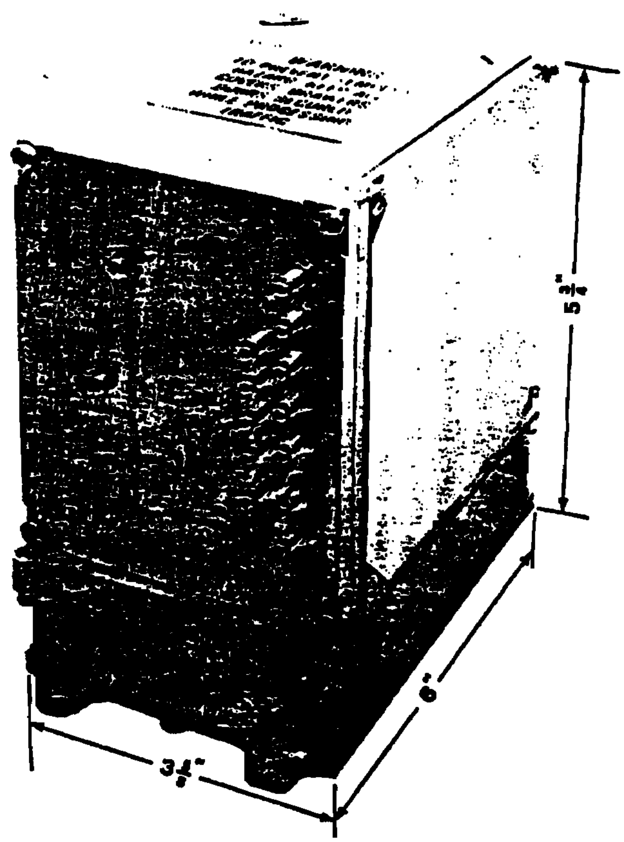
We have also talked of a number of electro-mechanical equipments that are dead or dying: one-time tape systems, and the KO-6 with its geared timing mechanism being most representative.

The variety of systems which have evolved has stemmed from needs for more efficiency, speed, security and the like: but, more fundamentally, from (1) the need to encrypt different kinds of information—literal traffic, TTY, data, facsimile, TV, and voice, (2) the need to suit encryption systems to a variety of communications means—wire lines, narrow-band and broad-band radio circuits, single-channel and multiplex communications, tactical and fixed-plant communications facilities; and (3) the need to suit these systems to a variety of physical environments.

*Specialized Systems.*—There are two other types of systems now in the inventory beyond those I have described that I want to touch on briefly. I have left them till last because they are among the most specialized and have as yet seen relatively little use in comparison with the big systems we have talked about. The first of these is the KG-24, designed for the encryption of TV signals—civision we call it. With the requirement for encrypting TV signals, we found ourselves faced with the problem of generating key at extremely high speeds, even by computer standards. So far, the fastest system I have described to you was the old AFSAY-816 with a bit-rate of 320 KHz—but this took six bays of equipment and had security, operational, and maintenance problems almost from the outset. Among the modern systems, the KG-3/13, with bit rates up to 100 kilobits was the fastest. But, as you know, with your home TV set, you tune to megahertz instead of kilohertz and it takes millions of bits each second to describe and transmit these TV signals. The KG-24 does it, and in one fairly large cabinet. [redacted] But there are only 6 (V-1) and 7 (V-2) models in existence, and further procurement is not planned. The main thing wrong with it is simply that it costs much too much.

The second type of modern specialized system I want to talk about is the family of equipment designed specifically to go into space vehicles. There were some obvious and some not-so-obvious difficulties that had to be met in the design of these equipments. One obvious problem was to make them small enough, and this requirement gave a big push to our general work in the micro-miniaturization of hardware. The second problem was also inherent in space technology—that was the need for extreme reliability. For unmanned surveillance satellites, if the system fails, you can't call a maintenance man. So we were faced with more rigid specifications and quality controls than we had ever seen before. The third problem has to do with the extraordinary complexity of satellite systems as a whole. We have found it next to impossible to provide decent crypto-equipment for our customers without a very full understanding of the whole communications and operations complex in which they are to operate. With our limited manpower, this has proven difficult enough to do with modern conventional communications systems and switching complexes on the ground but, for the space requirements, we had to educate our people to speak and understand the language of this new technology; and we have a little group who live and breathe this problem to the exclusion of nearly everything else.

And finally, we had to throw a lot of our basic *methodology* out the window. Every machine I have talked to you about so far, without exception, is built to have some of its variables changed at least once each day, and some of them more often. Everyone of them is classified and *accountable*: can you imagine how a crypto-custodian, charged with the specific responsibility of vouching for the whereabouts of a classified machine or classified key felt upon watching one of his precious items go rocketing off into space? Of course, we decided that we ought to "drop" accountability at the time of loss, although "lift" accountability might have been a more appropriate term. In any event, here's one of these key generators we use in space:



What we built into it was a principle that would put out a key that would not repeat itself for a very long period of time—weeks or months or years, whatever was required. Actually, with many of these new key generators, the matter of assuring a very long unrepeated sequence or, as we call it, a *long cycle*, is not so difficult. Even something as the KO–6 with its geared timing mechanism and just six metal disks would run full tilt for something like 33 years before the disks would reach

EO 1.4.(c)



eir original alignment again, and the daily change of its key was incorporated mainly to limit the scope of any loss that might occur—that business of supersession and compartmentation again. [redacted] So far, these things are working well—one technical security problem has been encountered. [redacted]

We have several such systems now. We don't talk about them very much because the whole question of surveillance satellites is a very sensitive one and, of course, that's what these are used for.

Before moving on, there are a few more things you ought to know about the nomenclature system and the equipment development cycle we have touched on from time to time already. The first point is that the TSEC nomenclature we have is *not* assigned to an equipment until it has been worked on by R&D for some time and they have done feasibility studies and have, perhaps, hand-made all or portions of it to figure out the circuitry or mechanical linkages to see if the thing will work. These very early versions are called "bread-board" models, and are likely to bear little or no resemblance to the final product. R&D assigns cover names to these projects in order to identify them conveniently—the only clue to the nature of the beast involved is contained in the first letter of what ever name they assign. The letters generally correspond to the equipment-type designator in the TSEC scheme—with "W" standing for TTY, "Y" for ciphony, etc. So, in the early R&D stage, "YACKMAN" stood for a voice equipment; "WALLER" for a TTY equipment, "GATLING" for a generator, etc.

When it looks like a development is going to come to fruition, TSEC nomenclature is assigned, and *suffixes* are added to the basic designators to indicate the stage reached in each model: these can involve experimental models (designated X), development models (designated D), test models (T), pre-production models (P), and finally, with the first full scale production model, no suffix at all.

So there could have been versions of the KW-26 successively called: W-; KW-26-X; KW-26-D; KW-26-T; KW-26-P, and the first operational equipment called merely KW-26. But, in fact, when some of the early models come out well enough, some of these stages may be skipped; in fact, most of them were with the KW-26, and it has been increasingly the trend to skip as many as possible to save time and money.

But this tortuous path of nomenclating does not end, even here. *After* the equipment gets into production, more often than not, some modifications need to be made to it and, when this occurs, we need some means of differentiating them, mainly for maintenance and logistical reasons, and the suffixes A, B, C, etc., are assigned. So, in fact, we now have four operational versions of the KW-26: the KW-26-A, the KW-26-B, KW-26-C, and KW-26-D.

EO 1.4.(c)

## TENTH LECTURE: TEMPEST

In 1962, an officer assigned to a very small intelligence detachment in Japan was performing the routine duty of inspecting the area around his little cryptocenter. As required he was examining a zone 200 ft. in radius to see if there was any "clandestine technical surveillance". Across the street, perhaps a hundred feet away, was a hospital controlled by the Japanese government. He sauntered past a kind of carport jutting out from one side of the building and, up under the eaves, noticed a peculiar thing—a carefully concealed dipole antenna, horizontally polarized, with wires leading through the solid cinderblock wall to which the carport abutted. He moseyed back to his headquarters, then quickly notified the counter-intelligence people and fired off a report of this "find" to Army Security Agency, who, in turn, notified NSA. He was directed to examine this antenna in detail and perhaps recover it, but although the CIC had attempted to keep the carport under surveillance that night, the antenna had mysteriously disappeared when they checked the next day. Up on the roof of the hospital was a forest of Yagi's, TV-antennas, all pointing towards Tokyo in the normal fashion, except *one*. That one was aimed right at the U.S. cryptocenter.

[redacted]

Why, back in 1954, when the Soviets published a rather comprehensive set of standards for the suppression of radio frequency interference, were those standards much more stringent for their teletypewriters and other communications equipment than for such things as diathermy machines, industrial motors, and the like, even though the teleprinters were much quieter in the first place?

Behind these events and questions lies a very long history beginning with the discovery of a possible threat, the slow recognition of a large number of variations of that threat and, lumbering along a few months or a few years afterwards, a set of countermeasures to reduce or eliminate each new weakness that has been revealed. I am going to devote several hours to this story, because your exposure to this problem may be only peripheral in your other courses, because it has considerable impact on most of our cryptosystems, and because we view it as the most serious technical security problem we currently face in the COMSEC world.

First, let me state the general nature of the problem as briefly as I can, then I will attempt something of a chronology for you. In brief: any time a machine is used to process classified information electrically, the various switches, contacts, relays, and other components in that machine may emit radio frequency or acoustic energy. These emissions, like tiny radio broadcasts, may radiate through free space for considerable distances—a half mile or more in some cases. Or they may be induced on nearby conductors like signal lines, power lines, telephones lines, or water pipes and be conducted along those paths for some distance—and here we may be talking of a mile or more.

When these emissions can be intercepted and recorded, it is frequently possible to analyze them and recover the intelligence that was being processed by the source equipment. The phenomenon affects not only cipher machines but *any* information-processing equipment—teleprinters, duplicating equipment, intercomms, facsimile, computers—you name it. But it has special signifi-

-cance for cryptomachines because it may reveal not only the plain text of individual messages being processed, but also that carefully guarded information about the internal machine processes being governed by those precious keys of ours. Thus, conceivably, the machine could be radiating information which could lead to the reconstruction of our key lists—and that is absolutely the worst thing that can happen to us.

Now, let's go back to the beginning. During WW II, the backbone systems for Army and Navy secure TTY communications were one-time tapes and the primitive rotor key generator then called SIGTOT. Bell Telephone rented and sold the military a mixing device called a 131-B2 and this combined with tape or SIGTOT key with plain text to effect encryption. They had one of these mixers working in one of their laboratories and, quite by accident, noted that each time the machine stepped, a spike would appear on an oscilloscope in a distant part of the lab. They examined these spikes more carefully and found, to their real dismay, that they could read the plain text of the message being enciphered by the machine. Bell Telephone was kind enough to give us some of their records of those days, and the memoranda and reports of conferences that ensued after this discovery are fascinating. They had sold the equipment to the military with the assurance that it was secure, but it wasn't. The only thing they could do was to tell the Signal Corps about it, which they did. There they met the charter members of a club of skeptics (still flourishing!) which could not believe that these tiny pips could really be exploited under practical field conditions. They are alleged to have said something like: "Don't you realize there's a war on? We can't bring our cryptographic operations to a screeching halt based on a dubious and esoteric laboratory phenomenon. If this is really dangerous, prove it." The Bell engineers were placed in a building on Varick Street in New York. Across the street and about 80 feet away was Signal Corps' Varick Street cryptocenter. The Engineers recorded signals for about an hour. Three or four hours later, they produced about 75% of the plain text that was being processed—a fast performance, by the way, that has rarely been equalled. (Although, to get ahead of the story for a moment, in some circumstances now-a-days, either radiated or conducted signals can be picked up, amplified, and used to drive a teletypewriter directly thus printing out the compromising information in real time.)

The Signal Corps was more than somewhat shook at this display and directed Bell Labs to explore this phenomenon in depth and provide modifications to the 131-B2 mixer to suppress the danger. In a matter of six months or so, Bell Labs had identified three separate phenomena and three basic suppression measures that might be used. The first two phenomena were the space radiated and conducted signals I have described to you; the third phenomenon was magnetic fields. Maybe you remember from high school physics having to learn about left hand rule of thumb and right hand rule of thumb, and it had to do with the fact that a magnetic field is created around a wire every time current flows. Well, a prime source of radiation in an old-fashioned mixing device is a bank of magnet-actuated relays that open and close to form the elements of teletypewriter characters being processed. The magnetic fields surrounding those magnets expand and collapse each time they operate, so a proper antenna (usually some kind of loop, I think) nearby can detect each operation of each relay and thus recover the characters being processed. The bad thing about magnetic fields is that they exist in various strengths for virtually all the circuitry we use and are extremely difficult to suppress. The good thing about them is that they "attenuate" or decay rapidly. Even strong fields disappear in 30 feet or so, so they comprise a threat only in special circumstances where a hostile intercept activity can get quite close to us.

The three basic supression measures Bell Labs suggested were:

1. Shielding (for radiation through space and magnetic fields),
2. Filtering (for conducted signals on power lines, signal lines, etc),
3. Masking (for either space radiated or conducted signals, but mostly for space).

The trouble with these solutions, whether used singly or in combination, all stems from the same thing: that is the fact that, quite typically, these compromising emanations may occur over a very large portion of the frequency spectrum, having been seen from near d.c. all the way up to the gigacycle range (and that's a lot of cycles). Furthermore, 5 copies of the same machine may each exhibit different characteristics, radiating at different frequencies and with different amplitudes. And even the same machine may change from day to day as humidity changes or as contacts become pitted, or as other components age. This means that any shielding used must form an effective barrier against a large variety of signals, and this proves difficult. Similarly, the filter has to be a nearly perfect one and they become big, heavy, and expensive. Furthermore, on signal lines for example, how do you get your legitimate cipher signal through without compromising signals squeezing through with them?

Masking, which is the notion of deliberately creating a lot of ambient electrical noise to override, jam, smear out or otherwise hide the offending signals, has its problems too. It's very difficult to make a masking device which will consistently cover the whole spectrum, and the idea of deliberately generating relatively high amplitude interference does not sit too well with folks like IRAC (The Interdepartmental Radio Advisory Committee) of the Office of Telecommunications (OTP) who don't like the idea of creating herring bone patterns in nearby TV pictures or interrupting legitimate signals like aircraft beacons.

Bell Labs went ahead and modified a mixer, calling it the 131-A1. In it they used both shielding and filtering techniques. Signal Corps took one look at it and turned thumbs down. The trouble was, to contain the offending signals, Bell had to virtually encapsulate the machine. Instead of a modification kit that could be sent to the field, the machines would have to be sent back and rehabilitated. The encapsulation gave problems of heat dissipation, made maintenance extremely difficult, and hampered operations by limiting access to the various controls.

Instead of buying this monster, the Signal Corps people resorted to the only other solution they could think of. They went out and warned commanders of the problem, advised them to control a zone about 100 feet in diameter around their communications center to prevent covert interception, and let it go at that. And the cryptologic community as a whole let it go at that for the next seven years or so. The war ended; most of the people involved went back to civilian life; the files were retired, dispersed, and destroyed. The whole problem was plain forgotten. Then, in 1951, the problem was, for all practical purposes, rediscovered by CIA when they were toying with the same old 131-B2 mixer. They reported having read plain text about a quarter mile down the signal line and asked if we were interested. Of course, we were. Some power line and signal line filters were built and immediately installed on these equipments and they did the job pretty well as far as conducted signals were concerned. Space radiation continued unabated, however, and the first of many "radiation" policies was issued in the form of a letter (AFSA Serial: 000404, Nov. 1953?) to all SIGINT activities requiring them to either:

1. Control a zone 200 feet in all directions around their cryptocenters (the idea of preventing interceptors from getting close enough to detect space radiation easily), or
2. Operate at least 10 TTY devices simultaneously (the idea of masking; putting out such a profusion of signals that interception and analysis would be difficult), or
3. Get a waiver based on operational necessity.

And the SIGINT community conformed as best it could; and general service communicators adopted similar rules in some instances. The 200 feet figure, by the way, was quite arbitrary. It was not based on any empirical evidence that beyond such distance interception was impractical. Rather, it was the biggest security zone we believed the majority of stations could reasonably comply with and we knew that, with instrumentation then available, successful exploitation at that range was a darn sight more difficult than at closer distances and, in some environments not practical at all.

At the same time we were scurrying around trying to cope with the 131-B2 mixer, we thought it would be prudent to examine every other cipher machine we had to see whether the same problem existed. For, way back in the late 40's, Mr. Ryon Page and one of his people were walking past the cryptocenter at Arlington Hall and had heard the rotor machines inside clunking away. He wondered what the effect would be on the security of those systems if someone were able to determine which rotors or how many rotors were stepping during a typical encryption process. In due course, some assessments were made on what the effect would be. The assessments concluded that it would be bad, and they were filed away for future reference. Now, it appeared that there might be a way for an interceptor to recover this kind of data. So, painstakingly, we began looking at our cryptographic inventory. Everything tested radiated and radiated rather prolifically. In examining the rotor machines, it was noted the voltage on their power lines tended to fluctuate as a function of the numbers of rotors moving, and so a fourth phenomenon, called power line modulation, was discovered through which it was possible to correlate tiny surges and drops in power with rotor motion and certain other machine functions.

Progress in examining the machines and developing suppression measures was very slow. In those days, S2 did not have any people or facilities to work on this problem; no fancy radio receivers or recording devices, no big screen rooms and other laboratory aids, and such things as we obtained we begged from the SIGINT people at Ft. Meade. In due course, they got overloaded, and they could no longer divert their SIGINT resources to our COMSEC problems. So R&D began to pick up a share of the burden, and we began to build up a capability in S2. The Services were called in, and a rudimentary joint program for investigative and corrective action got underway. The Navy, particularly, brought considerable resources to bear on the problem.

By 1955, a number of possible techniques for suppressing the phenomena had been tried: filtering techniques were refined somewhat; teletypewriter devices were modified so that all the relays operated at once so that only a single spike was produced with each character, instead of five smaller spikes representing each baud—but the size of the spike changed with each character produced and the analysts could still read it quickly. A "balanced" 10-wire system was tried which would cause each radiated signal to appear identical, but to achieve and maintain such balance proved impractical. Hydraulic techniques were tried to get away from electricity, but were abandoned as too cumbersome; experiments were made with different types of batteries and motor generators to lick the power line problem—none too successfully. The business of discovering new TEMPEST threats, of refining techniques and instrumentation for detecting, recording, and analyzing these signals progressed more swiftly than the art of suppressing them. With each new trick reported to the bosses for extracting intelligence from cryptomachines and their ancillaries, the engineers and analysts got the complaint: "Why don't you guys stop going onward and upward, and try going downward and backward for a while—cure a few of the ills we already know about, instead of finding endless new ones." I guess it's a characteristic of our business that the attack is more exciting than the defense. There's something more glamorous, perhaps, about finding a way to read one of these signals a thousand miles away than to go through the plain drudgery and hard work necessary to suppress that whacking great spike first seen in 1943.

At any rate, when they turned over the next rock, they found the acoustical problem under it. Phenomenon #5. Of course, you will recall Mr. Page and his people speculating about it way back in 1949 or so, but since the electromagnetic phenomena were so much more prevalent and seemed to go so much farther, it was some years before we got around to a hard look at what sonic and ultrasonic emissions from mechanical and electromechanical machines might have in store.

We found that most acoustical emanations are difficult or impossible to exploit as soon as you place your microphonic device outside of the room in which the source equipment is located: you need a direct shot at the target machine; a piece of paper inserted between, say an offending keyboard, and the pickup device is usually enough to prevent sufficiently accurate recordings to permit exploitation. Shotgun microphones—the kind used to pick up a quarterback's signals in a huddle—and large parabolic antennas are effective at hundreds of feet if, again, you can see the equipment. But in general, the acoustical threat is confined to those installations where the covert interceptor has been able to get some kind of microphone in the same room with your information-processing device—some kind of microphone like an ordinary telephone that has been bugged or left off the hook. One interesting discovery was that, when the room is "soundproofed" with ordinary acoustical title, the job of exploitation is easier because the soundproofing cuts down reflected and reverberating sound, and thus provides cleaner signals. A disturbing discovery was that ordinary microphones, probably planted for the purpose of picking up conversations in a cryptocenter, could detect machine sounds with enough fidelity to permit exploitation. And such microphones were discovered in [redacted]

The example of an acoustical intercept I just showed you is from an actual test of the little keyboard of the KL-15. You will note that each individual key produces a unique "signature". Since (before it died) the KL-15 was expected to be used in conjunction with telephonic communications, this test was made by placing the machine a few feet from a gray phone handset at Ft. Meade and making the recording in the laboratory at Nebraska Avenue from another handset. So that's really a recording taken at a range of about 25 miles, and the signals were encrypted and decrypted in the gray phone system, to boot.

The last but not least of the TEMPEST phenomena which concerns us is referred to as cipher signal modulation or, more accurately, as cipher signal anomolies. An anomaly, as you may know, is a peculiarity or variation from the expected norm. The theory is this: suppose, when a crypto-system is hooked to a radio transmitter for on-line operation, compromising radiation or conducted signals get to the transmitter right along with the cipher text and, instead of just sending the cipher text, the transmitter picks up the little compromising emissions as well and sends them out full blast. They would then "hitchhike" on the cipher transmission, modulating the carrier, and would theoretically travel as far as the cipher text does. Alternatively, suppose the compromising emanations cause some tiny variations or irregularities in the cipher characters themselves, "modulate" them, change their shape or timing or amplitude? Then, possibly, anyone intercepting the cipher text (and anyone can) can examine the structure of the cipher signals minutely (perhaps by displaying and photographing them on the face of an oscilloscope) and correlate these irregularities or anomalies with the plain text that was being processed way back at the source of the transmission. This process is called "fine structure analysis". Clearly, if this phenomenon proves to be at all prevalent in our system, its implications for COMSEC are profound. No longer are we talking about signals which can, at best, be exploited at perhaps a mile or two away and, more likely, at a few hundred feet or less. No longer does the hostile interceptor have to engage in what is really an extremely difficult and often dangerous business, i.e., getting covertly established close to our installations, working with equipment that must be fairly small and portable so that his receivers are unlikely to be ultra-sensitive, and his recording devices far less than ideal. Rather, he may sit home in a full-scale laboratory with the most sophisticated equipment he can assemble and, with plenty of time and no danger carry out his attack. But, so far, we seem to be all right. For several years, we have had SIGINT stations collecting samples of U.S. cipher transmissions containing possible anomalies and forwarding them here for detailed examination. We have no proven case of operational traffic jeopardized this way. [redacted]

I believe we've talked enough about the difficulties we face.

In late 1956, the Navy Research Laboratory, which had been working on the problem of suppressing compromising emanations for some years, came up with the first big breakthrough in a suppression technique. The device they produced was called the NRL Keyer, and it was highly successful. After being confronted with the shortcomings of shields and filters and maskers, they said, "Can we find a way of eliminating these offending signals at their source? Instead of trying to bottle up, filter out, shield, mask, or encapsulate these signals, why not reduce their amplitudes so much that they just can't go very far in the first place? Can we make these critical components operate at one or two volts instead of 60 or 120, and use power measured in microamps instead of milliamps?" They could, and did. NSA quickly adopted this low-level keying technique and immediately produced several hundred one-time tape mixers using this circuitry, together with some nominal shielding and filtering. The equipment was tested, and components that previously radiated signals which were theoretically exploitable at a half mile or so could no longer be detected at all beyond 20 feet. The next equipment built, the KW-26, and every subsequent crypto-equipment produced by this Agency contained these circuits, and a great stride had been made.

But we weren't out of the woods yet: the communicators insisted that the reduced voltages would give reduced reliability in their equipments, and that while satisfactory operation could be demonstrated in a simple setup with the crypto-machine and its input-output devices located close by, if the ancillaries were placed at some distance ("remoted" they call it), or if a multiplicity of ancillaries had to be operated simultaneously from a single keyer, or if the low level signals had to be patched through various switchboard arrangements, operation would be unsatisfactory. The upshot was that in the KW-26 and a number of other NSA machines, an "option" was provided—so that either high-level radiating signals could be used or low-level keying adopted. In the end, almost all of the installations were made without full suppression. Even the CRITICOM network, the key intelligence reporting system over which NSA exercises the most technical and operational control, was engineered without full-scale, low-level keying.

The next difficulty we found in the corrective action program was the great difference in cost and efficiency between developing new relatively clean equipment by incorporating good suppression features in the basic design, and in retrofitting the tens of thousands of equipments—particularly the ancillaries such as teletypewriters—which we do not build ourselves but, rather, acquire from commercial sources. For, in addition to the need for low-level keyers, some shielding and filtering is still normally required; circuits have to be laid out very carefully with as much separation or isolation as possible between those which process plain text and those which lead to the outside world—this is the concept known as Red/Black separation, with the red circuits being those carrying classified plain text, and the other circuits being black. Finally, grounding had to be very carefully arranged, with all the red circuits sharing a common ground and with that ground isolated from any others. To accomplish this task in an already established installation is extremely difficult and costly, and I'll talk about it in more detail later when I cover the basic plans, policies, standards, and criteria which have now been adopted.

By 1958, we had enough knowledge of the problem, possible solutions in hand, and organizations embroiled to make it possible to develop some broad policies with respect to TEMPEST. The MCEB (Military Communications Electronics Board) operating under the JCS, formulated and adopted such policy—called a Joint policy because all the Services subscribed to it. It established some important points:

1. As an *objective*, the Military would not use equipment to process classified information if it radiated beyond the normal limits of physical control around a typical installation.

2. *Fifty feet* was established as the normal limit of control. The choice of this figure was somewhat arbitrary; but *some* figures had to be chosen since equipment designers needed to have some upper limit of acceptable radiation to work against.

3. NAG-1, a document produced by S2, was accepted as the standard of measurement that designers and testers were to use to determine whether the fifty-foot limit was met. This document specifies the kinds of measurements to be made, the sensitivity of the measuring instruments to be used, the specific procedures to be followed in making measurements, and the heart of the document sets forth a series of *curves* against which the equipment tester must compare his results: if these curves are exceeded, radiated signals (or conducted signals, etc.) can be expected to be detectable *beyond* 50 feet, and added suppression is necessary.

4. The classification of various aspects of the TEMPEST problem was specified.

Documents like these are important. It was more than an assembly of duck-billed platitudes; it set the course that the Military would follow, and laid the groundwork for more detailed policies which would eventually be adopted nationally. It had weaknesses, of course. It said nothing about *money*, for example; and the best intentions are meaningless without budgetary action to support them. And it set no time frame for accomplishing the objective. And it provided no priorities for action, or factors to be used in determining which equipments, systems, and installations were to be made to conform first.

The next year, 1959, the policy was adopted by the Canadians and UK, and thus became a Combined policy. This gave it a little more status, and assured that there would be a consistent planning in systems used for Combined communications. In that same year, the first National COMSEC Plan was written. In it, there was a section dealing with compromising emanations. This document was the first attempt to establish some specific responsibilities among various agencies of Government with respect to TEMPEST, and to lay out an orderly program of investigative and corrective action. Based on their capabilities and interest, six organizations were identified to carry out the bulk of the work. These were ourselves, Navy, Army, Air Force, CIA, and State. The plan also called for some central coordinating body to help manage the overall effort. It was also in this plan that, for the first time, there were really explicit statements made indicating that the TEMPEST problem was not confined to communications security equipment and its ancillaries, that it extended to *any* equipment used to process classified information, including *computers*.

And so, it was in about this time frame that the word began to leak out to people outside the COMSEC and SIGINT fields, to other agencies of government, and to the manufacturing world.

You may remember from your briefings on the overall organization of this Agency, that there is something called the U.S. Communications Security Board, and that very broad policy direction for all COMSEC matters in the government stems from the Board. It consists of a chairman from the Dept. of Defense through whom the Director, NSA reports to the Secretary of Defense, and members from NSA, Army, Navy, Air Force, State, CIA, FBI, AEC, Treasury and Transportation. This Board meets irregularly, it does its business mainly by circulating proposed policy papers among its members and having them vote for adoption. The USCSB met in 1960 to contemplate this TEMPEST problem, and established its first and only permanent committee to cope with it. This committee is referred to as SCOCE (Special Committee on Compromising Emanations) and has, to date, always been chaired by a member of the S Organization.

The ink was hardly dry on the committee's charter before it got up to its ears in difficulty. The counterpart of USCSB in the intelligence world is called USIB—the U.S. Intelligence Board. Unlike USCSB, it meets regularly and has a structure of permanent committees to work on various aspects of their business. One part of their business, of course, consists of the rapid processing, by computer techniques, of a great deal of intelligence, and they had been contemplating the adoption of some standardized input-output devices of which the archetype is an automatic electric typewriter called *Flexowriter* which can type, punch tapes or cards, and produce page copy, and which is a very strong radiator. In a rare action, the Intelligence Board appealed to the COMSEC Board for policy direction regarding the use of these devices and, of course, this was immediately turned over to the fledgling Special Committee. The committee arranged to have some Flexowriters and similar equipments tested. They were found, as a class, to be the strongest emitters of space radiation of any equipment in wide use for the processing of classified information. While, as I have mentioned, typical unsuppressed teletypewriters and mixers are ordinarily quite difficult to exploit much beyond 200 feet through free space, actual field tests to Flexowriters showed them to be readable as far out as 3,200 feet and, typically, at more than 1000 feet, even when they were operated in a very noisy electrical environment.

One such test was conducted at the Naval Security Station. (By the way, in case I haven't mentioned this already, the S Organization was located at the Naval Security Station, Washington D.C. until May 1968 when we moved here to Ft. Meade.) Mobile test equipment had been acquired, including a rolling laboratory which we refer to as "the Van". In S3, a device called *Justowriter* was being used to set up maintenance manuals. Our van started out close to the building and gathered in a great potpourri of signals emitting from the tape factory and the dozens of the machines operating in S3. As they moved out, most of the signals began to fade. But not the Justowriter. By the time they got out to the gas station on the far side of the parking lot—that's about 600 feet—most of the other signals had disappeared, but they could still read the Justowriter. They estimated that the signals were strong enough to have continued out as far as American University grounds three blocks away. (The solution in this case, was to install a shielded enclosure—a subject I will cover subsequently.)

In any event, the Committee submitted a series of recommendations to the USCSB which subsequently became known as the *Flexowriter Policy*. The Board adopted it and it upset everybody. Here's why: as the first point, the Committee recommended that the existing Flexowriters not be used to process classified information at all in any overseas environment; that it be limited to the processing of CONFIDENTIAL information in the United States, and then only if a 400-foot security zone could be maintained around it. Exceptions could be made if the equipment could be placed in an approved shielded enclosure, or as usual, if waivers based on operational necessity were granted by the heads of the departments and agencies concerned.

The Committee also recommended that both a "quick-fix" program and a long-range, corrective action program be carried out. It was recommended that the Navy be made Executive Agent to develop a new equipment which would meet the standards of NAG-1 and, grudgingly, DDR&E gave Navy some funds (about a quarter of what they asked for) to carry out that development. Meanwhile, manufacturers were coaxed to develop some interim suppression measures for their product lines, and the Committee published two lists: one containing equipments which were forbidden, the other specifying acceptable interim devices. This policy is still in force; but most users have been unable to afford the fixes, and have chosen to cease operations altogether, e.g., CIA, or to operate under waivers on a calculated risk basis, e.g., most SIGINT sites.

While the Committee was still reeling from the repercussions and recriminations for having sponsored an onerous and impractical policy which made it more difficult for operational people to do their job, it grasped an even thornier nettle. It undertook to take the old toothless Joint and Combined policies and convert them into a strong National policy which:

1. Would be binding on all departments and agencies of government, not just the military.
2. Would establish NAG-1 as a standard of acceptance for future government procurement of hardware (NAG-1, by the way, was converted to *Federal Standard*. (FS-222) to facilitate its wide distribution and use.)
3. Would establish a deadline for eliminating unsuppressed equipment from government inventories.

By now the governmental effort had changed from a haphazard, halting set of uncoordinated activities mainly aimed at cryptologic problems, to a multi-million dollar program aimed at the full range of information-processing equipment we use. Symposia had been held in Industrial forums to educate manufacturers about the nature of the problem and the Government's intentions to correct it. Work had been parcelled out to different agencies according to their areas of prime interest and competence; the SIGINT community had become interested in possibilities for gathering intelligence through TEMPEST exploitation. It, nonetheless, took the Committee two full years to complete the new National policy and coordinate it with some 22 different agencies. Before it could have any real effect it had to be *implemented*. The implementing directive—5200.19—was signed by Secretary McNamara in December, 1964. Bureaucracy is wonderful. Before its specific provisions could be carried out, the various departments and agencies had to implement the implementing directive within their own organizations. These implementing documents began dribbling in throughout 1965, and it is my sad duty to report that NSA's own implementation did not take effect until June, 1966.

All this makes the picture seem more gloomy than it is. These implementing documents are, in the final analysis, formalities. The fact of the matter is that most organizations, our own included, have been carrying out the intent of these policies to the best of our technical and budgetary abilities for some years.

While all this was going on in the policy field, much was happening in the technical area. First, let me cover the matter of shielded enclosures. To do so, I have to go back to about 1956 when the National Security Council got aroused over the irritating fact that various counter-intelligence people, particularly in the Department of State, kept stumbling across hidden microphones in their residences and offices overseas. They created a Technical Surveillance Countermeasures Committee under the Chairmanship of State and with the Services, FBI, CIA, and NSA also represented. This group was charged with finding out all they could about these listening devices,

EO 1.4.(c)

and developing a program to counter them. In the space of a few years, they assembled information showing that nearly 500 microphones had been discovered in U.S. installations; *all* of them overseas, 90% of those behind the [redacted] They examined a large number of possible countermeasures, including special probes and search techniques, electronic devices to locate microphones buried in walls, and what-have-you. Each June, in their report to the NSC, they would dutifully confess that the state-of-the-art of hiding surveillance devices exceeded our ability to find them. About the only way to be sure an [redacted] was "clean" would be to take it apart inch-by-inch which we couldn't afford, and which might prove fruitless anyhow, since host-country labor had to be used to put it back together again. (Incidentally, years later, we began to think we had darned well better be able to afford something close to it, for we found things that had been undetected in a dozen previous inspections.)

OGA

The notion of building a complete, sound-proof, inspectable room-within-a-room evolved to provide a secure conference area for [redacted] and intelligence personnel. During these years, NSA's main interest in and input to the committee had to do with the sanctity of cryptocenters in these vulnerable overseas installations, and we campaigned for rooms that would be not only sound-proof but proof against compromising electromagnetic emanations as well. [redacted] developed a conference room made of plastic which was dubbed the "fish-bowl" and some of them are in use behind the [redacted] now. CIA made the first enclosure which was both "sound-proof" and electrically shielded. This enclosure went over like—and apparently weighed about as much as—a lead balloon. It was nicknamed the "Meat Locker" and the consensus was that nobody would consent to work in such a steel box, that they needed windows and drapes or they'd get claustrophobia or something. Ironically, though, it turned out that some of the people who were against this technique for aesthetic reasons spent their days in sub-sub basement areas with cinder-block walls and no windows within 50 yards.

The really attractive thing about the enclosures, from the security point of view, was the fact that they provided not only the best means, but the only means we had come across to provide really complete TEMPEST protection in those environments where a large-scale intercept effort could be mounted at close range. So, despite aesthetic problems, and weight, and cost, and maintenance, and enormous difficulties in installation, we campaigned very strongly for their use in what we called "critical" locations, with [redacted] at the top of the list.

So again, in the matter of Standards, NSA took the lead, publishing two specifications (65–5 and 65–6) one describing "fully" shielded enclosures with both RF and acoustic protection; the other describing a cheaper enclosure providing RF protection only. And by threats, pleas, "proofs" and persuasion, we convinced the [redacted] CIA, and the Services, to procure a handful of these expensive, unwieldy screen rooms for installation in their most vulnerable facilities. One of the first, thank goodness, went into [redacted]—in fact, two of them; one for the [redacted] code room as they call it, and one for the cryptocenter used by the [redacted] So, when highest levels of government required us to produce damage reports on the microphone finds there, we were able with straight faces and good conscience to report that, in our best judgment, cryptographic operations were immune from exploitation—the fully shielded enclosures—were in place.

OGA

But none of us was claiming that this suppression measure was suitable for any wide-scale application—it's just too cramped, inflexible, and expensive. We have managed to have them installed not only in overseas installations where we are physically exposed but also in a few locations here at home where the information being processed is of unusual sensitivity. Thus, the [redacted] acquired more than 50 of them to house computers and their ancillaries where a heavy volume of Restricted Data must be processed; we have one here in S3 to protect most of our key and code generation equipment—a $134,000 investment, by the way—which you may see when you tour our production facilities. The Navy has one of comparable size at the Naval Security Station for its computers. (But they have the door open most of the time.) At Operations Building No. 1, on the other hand, we don't have one—instead, we use careful environmental controls, inspecting the whole area around the Operations Building periodically, and using mobile equipment to examine the actual radiation detectable in the area.

OGA

In about 1962, two more related aspects of the TEMPEST problem began to be fully recognized. First, there was the growing recognition of the inadequacies of suppression effort which were being made piece-meal, one equipment at a time, without relating that equipment to the complex of ancillaries and wiring in which it might work. We called this the "system" problem. We needed a way to test, evaluate, and suppress overall secure communications complexes, because radiation and conduction difficulties stem not only from the inherent characteristics of individual pieces of machinery but also from the way they are connected to other machines—the proximity and conductivity and grounding arrangements of all the associated wiring often determined whether a system as a whole was safe. And so, one of the first systems that we tried to evaluate in this way was the COMLOGNET system of the Army. This system, using the KG-13, was intended principally for handling logistics data and involved a number of switches, and data transceivers, and information storage units, and control consoles. Using the sharpest COMSEC teeth we have, our authority for reviewing and *approving* cryptoprinciples, and their associated rules, regulations, and procedures of use, we insisted that the system as a whole be made safe from the TEMPEST point of view before we would authorize traffic of all classifications to be processed. This brought enough pressure to bear on the system designers for them to set up a prototype complex at Ft. Monmouth and test the whole thing on the spot. They found and corrected a number of weaknesses before the "system" approval was given. A second means we have adopted, in the case of smaller systems, like a KW-7 being used with a teletypewriter and a transmitter distributor, is to pick a relatively small number of most likely configurations to be used and test each as a package. We clean up these basic packages as much as is needed and then approve them. If a user wants to use some less common arrangement of ancillaries, he must first test it. So, in the case of KW-7, we took the three most common teleprinters—the MOD-28 line of Teletype Corporation, the Kleinschmidt (an Army favorite), and the MITE teleprinter; authorized the use of any of these three combinations and provided the specific installation instructions necessary to assure that they would be radiation-free when used. We did the same thing with the little KY-8, this time listing "approved" radio sets with which it could be safely used.

Adequate systems testing for the larger complexes continues to be a problem—one with which S4, S2, DCA, and the Special Committee are all occupied.

The second and related problem that reared its head in about 1962 is the matter of RED/BLACK separation that I mentioned. Over the years, it had become increasingly evident that rather specific and detailed standards, materials, and procedures had to be used in laying out or modifying an installation if TEMPEST problems were to be avoided, and the larger the installation, the more difficult proper installation became—with switching centers perhaps the most difficult case of all. For some years, NSA has been making a really hard effort to get other organizations to display initiative and commit resources to the TEMPEST problem. We simply could not do it all ourselves. So we were pleased to cooperate with DCA when it decided to tackle the question of installation standards and criteria for the Defense Communications System (DCS). It was needed for all three Services; the Services, in fact, actually operate DCS. Virtually every strategic Department of Defense circuit is involved—more than 50,000 in all. DCA felt that this system would clearly be unmanageable unless the Services could standardize some of their equipment, communications procedures, signalling techniques, and the like. General Starbird, who directed DCA, was also convinced that TEMPEST is a serious problem, and desired the Services to use a common approach in DCS installations with respect to that problem. Thus, DCA began to write a very large installation standard comprising a number of volumes, and laying out in great detail how various circuits and equipments were to be installed. NSA personnel assisted in the technical inputs to this document called DCA Circular 175-6A. A Joint Study Group was formed under DCA chairmanship to coordinate the installation problem as well as a number of other TEMPEST tasks affecting the Defense Communications System and the National Communications System (NCS) which interconnects strategic civil organizations along with the Defense Department. In developing the installation standards, the study group and DCA took a rather hard line, and specified tough requirements for isolating all the RED circuits, equipments, and areas from the BLACK ones, i.e., assuring physical and electrical separation between those circuits carrying classified information in the clear, and those carrying only unclassified information (like cipher signals, control signals, power, and ordinary telephone lines). In addition to shielding and filtering, this called for the use of conduits and often, in existing installations, drastic rearrangement of all the equipment and wiring was involved.

You will remember that the Department of Defense had *directed* that extensive TEMPEST corrective action be taken. I said that the Directive specified NAG-1 (FS-222) as a standard of acceptance for new equipment. It also mentioned a number of other documents as being applicable, and particularly, this very same DCA Circular I've just been describing.

As this whole program gathered steam, the monetary implications began to look staggering; the capability of the government accomplishing *all* the corrective action implied in a reasonable time seemed doubtful: furthermore, we were beginning to see that there were subtle inter-relationships between different kinds of countermeasures; and that some of these countermeasures, in particular situations, might be quite superfluous when some of the other countermeasures were rigidly applied. Remember, by now we had been telling people to shield, to filter, to place things in conduit, to ground properly, to separate circuits, to use low-level keying, to provide security zones and sometimes, to use shielded enclosures. It took us a while to realize some fairly obvious things, for example, if you have done a very good job of suppressing space radiation, you may not need very much filtering of the signal line because there's no signal to induce itself on it; or you may not need to put that line in conduit for the same reason. If you have put a line in conduit, which is a kind of shielding, then perhaps you don't have to separate it very far from other lines because the conduit itself has achieved the isolation you seek. And so forth. We had already realized that some installations, inherently, have fewer TEMPEST problems than others. The interception of space radiation from an equipment located in a missile silo or SAC's underground command center does not seem practicable; so perhaps the expensive space radiation suppressions ought not be applied there. Similarly, the suppression measures necessary in an airborne platform or in a ship at sea are quite different from those needed in a communications center in Germany.

The upshot was that, in 1965, NSA undertook to examine all the standards and techniques of suppression that had been published, to relate them to one another, and to provide some guidelines on how the security *intent* of the "national policy" and its implementing directives could be met through a judicious and *selective* application of the various suppression measures as a function of installation, environment, traffic sensitivity, and equipment being used. These guidelines were published as NSA Circular 90-9 and have been extremely well received.

In December 1970, the U.S. TEMPEST community introduced new TEMPEST laboratory test standards for non-cryptographic equipments. Test procedures for compromising acoustical and electromagnetic emanations were addressed in two separate documents. These laboratory test standards were prepared by SCOCE and superseded FS-222. They were approved by the USCSB and promulgated as Information Memoranda under the National COMSEC/EMSEC Issuance System. NACSEM 5100 is the Compromising Emanations Laboratory Test Standard for Electromagnetic Emanations and NACSEM 5103 is the Compromising Emanations Laboratory Test Standard for Acoustic Emanations. These documents are intended only to provide for standardized testing procedures among U.S. Government Departments and Agencies. They were in no way intended to establish standardized TEMPEST suppression limits for all U.S. Government Departments and Agencies. Under the terms of the USCSB's National Policy on Compromising Emanations (USCSB 4-4), U.S. Government Departments and Agencies are responsible for establishing their own TEMPEST programs to determine the degree of TEMPEST suppression which should be applied to their information-processing equipments.

In January 1971, NSA published KAG-30A/TSEC, Compromising Emanations Standard for Cryptographic Equipments. This standard represented our first effort to establish standardized testing procedures and limits for controlling the level of compromising emanations from cryptographic equipments.

DCA Circular 175-6A was superseded by DCA Circular 300-175-1 in 1969, which in turn was replaced by MIL HDBK 232 on 14 November 1972.

Before I summarize the TEMPEST situation and give you my personal conclusions about its security implications, I should make it clear that there are a number of topics in this field which comprise additional problems for us beyond those I've talked about at length. There are, for example, about a half-dozen phenomena beyond the eight I described to you; but those eight were the most important ones. I have hardly touched on the role of industry or on the program designed to train manufacturers and mobilize their resources to work on the problem. I have mentioned on-site empirical testing of operating installations only in the case of Fort Meade—actually, each of the Services has a modest capability for checking out specific installations and this "mobile test program" is a valuable asset to our work in correcting existing difficulties. For example, the Air Force, Navy, and ourselves have completed a joint survey of the whole signal environment of the island of Guam. As you know, B52 and many Navy operations stage there. As you may not know, a Soviet SIGINT trawler has loitered just off-shore for many months. Are the Soviets simply gathering plain language communications, or are they able to exploit compromising emanations?

Another problem area is the matter of providing guidelines for the design of complete new government buildings in which they expect to use a good deal of equipment for processing classified information. How do we anticipate the *TEMPEST* problems that may arise and stipulate economical means for reducing them in the design and layout of the building itself? We consult with the architects for new federal office buildings, suggesting grounding systems and cable paths that will minimize TEMPEST suppression cost when they decide to install equipment.

Finally, equipment designers face some specific technical difficulties when certain kinds of circuits have to be used, or when the system must generate or handle pulses at a very high bit rate. These difficulties stem from the fact that these pulses are characterized by very fast "rise-times". They peak sharply, and are difficult to suppress. When this is coupled with the fact that on, say, a typical printed circuit board, there just isn't room to get this physical separation between lots of wires and components that ought to be isolated from one another, then mutual shielding or electrical "de-coupling" is very difficult. R&D has published various design guides to help minimize these problems, but they continue to add cost and time to our developments. With crypto-equipment, problems can be particularly acute because, almost by definition, any cryptomachine forms an interface between RED (classified) signals, and BLACK (unclassified) ones, for you deliver plain text to it, and send cipher text out of it—so the notion of RED/BLACK signal separation gets hazy in the crucial machinery where one type of signal is actually converted to the other.

## SUMMARY

We have discussed eight separate phenomena and a host of associated problems. We have identified a number of countermeasures now being applied, the main ones being the use of low-level keying, shielding, filtering, grounding, isolation, and physical protective measures. We have traced a program over a period of more than 20 years, with almost all the advances having been made in the last decade, and a coherent national program having emerged only in the past few years. My own estimate of the overall situation is as follows:

1. We should be neither panicked nor complacent about the problem.
2. Such evidence as we have been able to assemble suggests that a few of our installations, but very few of them, are probably under attack right now. Our own experience in recovering actual intelligence from U.S. installations under field conditions suggests that hostile success, if any, is fragmentary, achieved at great cost and—in most environments—with considerable risk.
3. There remain a number of more economical ways for hostile SIGINT to recover intelligence from U.S. communications entities. These include physical recovery of key, subversion, and interception and analysis of large volumes of information transmitted in the clear. But during the next five years or so, as our COMSEC program makes greater and greater inroads on these other weaknesses, and especially as we reduce the amount of useful plain language available to hostile SIGINT, it is logical to assume that that hostile effort will be driven to other means for acquiring

intelligence as more economical and productive, including increased effort at TEMPEST exploitation. Already, our own SIGINT effort is showing a modest trend in that direction. As knowledge of the phenomenon itself inevitably proliferates, and as techniques for exploitation become more sophisticated because of ever-increasing sensitivity of receivers, heightening fidelity of recording devices, and growing analytical capabilities, the TEMPEST threat may change from a potential one to an actual one. That is, it will become an actual threat *unless* we have been able to achieve most of our current objectives to suppress the equipments we will then have in our inventory and to clean up the installations in which those equipments will be used.

# A HISTORY
## OF
# U.S. COMMUNICATIONS SECURITY (U)

## THE DAVID G. BOAK LECTURES

## VOLUME II

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755

The information contained in this publication will not be disclosed to foreign nationals or their representatives without express approval of the DIRECTOR, NATIONAL SECURITY AGENCY. Approval shall refer specifically to this publication or to specific information contained herein.

JULY 1981

CLASSIFIED BY NSA/CSSM 123-2
REVIEW ON 1 JULY 2001

TABLE OF CONTENTS

## INTRODUCTION

(U) The first volume of this work was completed in 1966, and except for a brief update in 1972 treating mainly our part in the failure in Vietnam, has remained essentially unchanged. The purpose of the ensuing essays is to provide some historical perspective on some of the trends, concepts, ideas, and problems which have either arisen in the past decade or so or have persisted from earlier times. The material is intended to be essentially non-technical, and is for relative newcomers in our business. Our nuts and bolts are treated in considerable depth in KAG 32B/TSEC. It is commended to readers seeking detail, particularly on how our systems work and the specifics of their application.

## POSTSCRIPT ON SURPRISE

(U) We've encountered no serious argument from anybody with the thesis that COMSEC – a key ingredient of OPSEC – may help achieve surprise, nor with the correlative assertion that fewer and fewer major activities can be planned and executed these days without a large amount of supporting communications to coordinate, command and control them, nor even with the assertion that, without security for those communications, surprise is highly unlikely.

~~(C)~~ But, with all that said and accepted by customers, we may still be faced with the quite legitimate question: "What is its value – How much is it worth?" Is a KY-38 the right choice over rounds of ammunition to an assault platoon? Or all the other trade-offs you can imagine when we cost money, take space, consume power, use people, complicate communications, or reduce their speed, range, reliability, capacity, or flexibility. Can we quantify its value? Rarely, I fear, because we can so seldom show the success or failure of some mission to have been categorically and exclusively a function of the presence or absence of COMSEC. Even in the drone anecdote related in the following OPSEC chapter, where we'd like to credit a few crypto-equipments with the savings of several hundred million dollars worth of assets, there were other contributors like improved drone maneuverability and command and control, and increased EW support to disrupt North Vietnam's acquisition radars.

(U) In a straight military context, however, we know of one major effort to quantify the value of surprise. Professor Barton Whaley of Yale undertook to measure success and failure in battle as a strict function of the degree of surprise achieved by one side or the other. He used Operations Research techniques in an exhaustive analysis of 167 battles fought over a period of many years in different wars. He confined his choice of battles to those in which there were relatively complete unit records available for both sides and chose them to cover a wide variety of conditions which might be construed to affect the outcome of battle – terrain, weather, numerical or technical superiority of one side or the other, offensive or defensive positioning, and so on.

(U) His measures for "success" were the usual ones: kill ratios, casualty ratios, ordnance expenditures, POW's captured, and terrain or other objectives taken. He found that, regardless of the particular measure chosen and the other conditions specified, success was most critically dependent on the degree of surprise achieved. He found:

| | *No. of cases* | *Average casualty ratio (friend : enemy)* |
|---|---|---|
| SURPRISE: | 87 | 1: 14.5 |
| NO SURPRISE: | 51 | 1: 1.7 |
| NO DATA: | 29 | |

(U) The above is contained in Professor Whaley's book (still in manuscript form) Strategem: Deception and Surprise in War, 1969, p. 192.

(U) When the extreme cases were removed, the average casualty ratios were still better than 1:5 where surprise was achieved, vs. 1:1 when it was not (*Ibid.* p. 194).

(U) He further asserts that, nuclear weapons and missile delivery systems "...raise the salience of surprise to an issue of survival itself..." (*Ibid.*, p. 207).

(U) These seem to be facts worth noting in persuading people that their investment in COMSEC will be a good one; they'll get their money back, and then some. I have to confess, however, that the analogy between Whaley's findings and what COMSEC can do is flawed. For, Dr. Whaley was a World War II deception expert, and he believed that the best way to achieve surprise is through deception rather than through secrecy.

THIS PAGE IS INTENTIONALLY BLANK

**OPSEC**

(U) Since earliest times, one of the basic principles of warfare has been surprise. In fact, some early Chinese writings on the subject are quite eloquent. A strong case can be made that, seen broadly, a major purpose of COMSEC – perhaps its overriding purpose – is to help achieve surprise by denying enemy foreknowledge of our capabilities and intentions. The principle applies not only to strategic and tactical military operations but to the fields of diplomacy, technology, and economic warfare as well. In fact, it extends to almost any adversarial or competitive relationship.

(U) Operations Security (OPSEC) is a discipline designed fundamentally to attain and maintain surprise, particularly in military operations. In fact, I have seen drafts of an Army update of their doctrine on Principles of Warfare in which OPSEC is formally recognized as a supporting factor in the treatment of surprise.

~~(S-CCO)~~ The history of OPSEC and our involvement in it flows along the following lines: By 1966, both intelligence sources and after-action reports had made it abundantly clear that the North Vietnamese had sufficient foreknowledge of ARC LIGHT (B–52) and ROLLING THUNDER (tactical aircraft) raids to render many of those operations ineffective. A concerted effort began in an attempt to determine the sources of that foreknowledge. To that end, JCS assembled a group which included DIA, the Services and ourselves. NSA was a player, both because SIGINT had been the source of some of the most convincing evidence of enemy foreknowledge and because communications insecurities were thought to be a prime candidate as the culprit.

~~(C-CCO)~~ Early on, the Group decided that an all-source effort should be made. Three basic potential sources for the foreknowledge were soon established – hostile SIGINT exploiting U.S. signals insecurities; HUMINT (Human Intelligence) in which agents could physically observe and report on the planning and execution of missions; and operations analysts deducing the nature of forthcoming activity from an examination of stereotypic (repetitive) patterns revealed by our past activity.

~~(C)~~ OPSEC emerged as a formal discipline when it was decided, I believe at the urging of NSA representatives, that a methodology should be devised which would *systematize* the examination of a given operation from earliest planning through execution: a multi-disciplinary team would be established to work in concert, rather than in isolation; and its membership would include experts in COMSEC, counter-intelligence, and military operations. They would look at the entire security envelope surrounding an operation, find the holes in that envelope, and attempt to plug them.

(U) A most important decision was made to subordinate this OPSEC function to an operations organization, rather than to intelligence, security, plans, or elsewhere. It was thought essential (and it proved out, in the field) that OPSEC not be viewed as a policing or IG (Inspector General) function because, if it was so perceived, operators might resent the intrusion, circle their wagons and not cooperate as the team dug into every step taken in launching an operation. Rather, they were to be an integral part of Operations itself, with one overriding goal – to make operations more effective.

(U) Operations organizations (the J–3 in Joint activities, G–3 or S–3 in Army, N–3 in Navy, and A–3 in Air Force) generally seem to be top dogs in military operations. They are usually the movers and shakers, and alliance with them can often open doors and expedite action. And so it was with the formal OPSEC organization.

~~(S)~~ In a remarkably swift action, the JCS established an OPSEC function to be located at CINCPAC (Commander in Chief, Pacific), shook loose 17 hard-to-get billets, and the OPSEC team known as the Purple Dragons was born. An NSA planner and analyst out of S1 was a charter member and was dispatched to the Pacific. The Dragons got added clout by being required to brief the Joint Chiefs of Staff and the President's Foreign Intelligence Advisory Board on their progress each 3 months. They were to support all operations, not just air strikes. They were given a free hand, travelled constantly all over the Pacific, more or less wrote their charter as they went along, and repeatedly pin-pointed the major sources of operations insecurity. Sometimes they were able to help a commander cure a problem on the spot; other problems were more difficult to fix. In the case of air strikes, three of the biggest difficulties stemmed from the need to notify

ICAO (International Civil Aeronautical Organization), other airmen, and US and allied forces of impending operations well before the fact.

~~(C)~~ Altitude reservations (ALTREV's) were filed with ICAO, and broadcast in the clear throughout the Far East. Notices to Airmen (NOTAM's) specified the coordinates and times of strikes so that they would not fly through those areas, and these notices were posted at U.S. air facilities everywhere. Plain language broadcasts (called Heavy Artillery Warnings) saturated South Vietnam specifying where B52 (ARC LIGHT) strikes were to take place. U.S. officials were obliged to notify and sometimes seek approval of South Vietnamese provincial officials so that they could warn villagers of the coming action.

~~(C)~~ Some of these problems associated with ARC LIGHT operations were eventually solved by blocking out large air corridors to a single point of entry into SVN airspace; the Heavy Artillery warnings, once transmitted hours before a strike, were withheld until 60 minutes or less before the time on target.

~~(S)~~ In general, set patterns of operations were rather prevalent in land, sea, and air activity. Ground attacks at dawn were the rule not the exception; hospital ships were pre-positioned off amphibious landing areas; there were runs on the PX before troops moved out of garrison to combat. Major movements of ground forces were preceded by weeks of predictable and observable activity, arranging logistics, setting up convoy routes and bivouacs, coordination with supported and supporting forces and so on. The failure to take COSVN (the North Vietnamese "Central Office for SVN" in the Parrot's Beak area of Cambodia) was almost certainly the result of the huge flurry of indicators of impending attack that preceded it by at least three days.

~~(C)~~ HUMINT vulnerabilities were pervasive. North Vietnamese and Viet Cong agents had infiltrated most of the country. Yet the Purple Dragons were never able to demonstrate that agent reporting was a dominant factor in enemy anticipation of U.S. action. Rather, communications insecurities emerged as the primary source of foreknowledge in fully two-thirds of the cases investigated. On occasion, a specific link or net was proven to be *the* source of foreknowledge of a given operation, at least for a time.

~~(S)~~ A classic case involved the drone reconnaissance aircraft deployed out of South Vietnam to overfly North Vietnam, gather intelligence, and return. By late 1966, the recovery rate on these drones had dropped to about 50%. This deeply concerned us, not only because of the loss of intelligence and of these expensive ($500K at the time) aircraft, but also because we were certain that North Vietnamese anti-aircraft assets could not possibly have enjoyed such success without fairly accurate foreknowledge on where these planes would arrive, at about what time, and at what altitude. The Purple Dragons deployed to SVN, and followed their usual step-by-step examination of the whole process involved in the preparations made for launch and recovery, and the configuration and flight patterns of the mother ship and the drones themselves, the coordination between launch and recovery assets, including the planning message exchanged. The mother ships staged out of Bien Hoa in the southern part of SVN; the recovery aircraft out of DaNang to the North. Within a few days, the Dragons zeroed in on a voice link between the two facilities. Over this link flowed detailed information, laying out plans several days and sometimes for a week or more in advance on when and where the drones would enter and egress from North Vietnam. The link was "secured" by a weak operations code; the messages were stereotyped, thus offering cryptanalytic opportunities, and their varying lengths and precedences offered opportunities for traffic analysis. In short, the North Vietnamese might be breaking it, or enough of it to get the vital where and when data they needed to pre-position their anti-aircraft assets (surface to air missiles, anti-aircraft batteries, and fighter aircraft) to optimize the chance of shootdown.

~~(S)~~ As a check, the Dragons manipulated some messages over the link, with fascinating results. (See the March and April 1979 issues of *CRYPTOLOG* for some further details on this account at somewhat higher classification than possible here.) The OpCode was replaced quickly with a pair of fully secure KW-26 equipments. Starting the next day, the loss rate dropped dramatically. A few months later, it began a sudden rise, suggesting that the North Vietnamese had discovered a new source of information. The Purple Dragons revisited, and reassessed the problem. This time they concluded that the unique call signs of the Mother Ships were being exploited. The call signs were changed, and losses fell again, for a few weeks. The final solution was to put NESTOR aboard, and again the loss rate dropped so drastically that, by the end of the drone activity, only one or two drones were lost to enemy action annually in contrast to as many as two or three a week in the early days.

~~(C)~~ OPSEC is slowly being institutionalized. OPSEC elements are established in the JCS and at most Unified and Specified Commands. Service organizations are turning increasingly to the discipline but not, as you might expect in peacetime, with great enthusiasm. We have a modest capability for OPSEC in S as well, used largely in support of joint activity or, on request, to assist other organizations. We have also looked inward with the OPSEC methodology in helping DDO maintain the secrecy of his operations, and as still another cut at the general problem or computer security in DDT. Results have been useful.

~~(C)~~ The principal innovation in OPSEC methodology since early times was the development in S1 of a decision analysis routine called VULTURE PROBE to quantify the value of various COMSEC measures by showing how the probability of an enemy's reaching his objectives is reduced as a function of the COMSEC steps we apply. This in turn helps us to decide which information most needs protection, and the relative significance of the many individual security weaknesses an OPSEC survey is likely to uncover.

THIS PAGE IS INTENTIONALLY BLANK

EO 1.4.(c)

## ORGANIZATIONAL DYNAMICS

~~(C)~~ The first Volume described a relatively simple, straightforward functional organization for COMSEC in NSA – the traditional R&D organization for system invention and development, an Engineering organization to manage the production of equipments in quantity, a Materials organization to supply supporting keys and other materials, a Doctrinal organization to approve and regulate use, and a few supporting Staffs. (Please, young people in the line, don't laugh at the sort shrift Staffs usually get in description of who does what. It is more likely than not that it will be to your career advantage to have such an assignment for at least a little while before you are done. I predict that then your perspective on their importance and value will change even though you may now percieve that they are mostly in the way – particularly if you are trying to get something/anything done in a hurry. In general, (but obviously not always) they enjoy the luxury and suffer the uncertainties of having time to think things through.

~~(C)~~ Our organizational structure changed over time, generally in response to changed requirements, priorities, and needed disciplines. Down in the noise somewhere (except in the scruffy gossip mill) were other factors like personalities, managerial competence, office politics, and so on. The original Doctrine/Engineering/Material triad survived for slightly more than 20 years. Exploding communications technology, quantum jumps in system complexity, speed, capacity, efficiency, reliability, and quantity left our engineers in R and S and our production people strangely unstressed. They had kept pace with technology breakthroughs over the years, and sometimes paced them.

~~(C)~~ The Doctrinal organization, however, was beginning to burst at the seams. Here was a group that had had little change in numerical strength since its inception, dominated by liberal artists except in cryptanalytic work, trying to cope with technologies so complex in the requirements world that they were hard put to understand, much less satisfy those requirements. A DoD Audit team found, in S, too great a concentration on the production of black boxes and made strong recommendations that we change to a "systems" approach to more fully integrate our cryptosystems into the communications complexes they support.

~~(C)~~ So, in 1971, came our first major re-organization and S4 (now S8) was born (out of Doctrine by Barlow). Its mission was to get cryptography *applied.* What seemed required was a cadre of professionals, including a liberal infusion of engineers, computer scientists, and mathematicians, in a single organization who would be the prime interface with our customers to define *system* security requirements and to assist in the integration of cryptography to that end. There were, of course, mixed emotions about dilution of our scarce technical talent into a kind of marketing operation, but it paid off.

[redacted]

~~(C)~~ A couple of years later (July 1974), another audit report recommended better centralized management and control of cryptographic assets in Government. The Acquisition staff was converted to a full scale line organization (S5) in part in response to that recommendation. There is a persistent view that the ability of an organization to get something done is inversely proportional to the number of people on staff. The

Marine Corps is the arch-type: lean and mean; lots of fighters, little excess baggage in the form of staffers – logisticians, budgeteers, planners, policy makers, clerks, typists, researchers, educators, administrators, and the like.

~~(C-NF)~~ A hoax, of course. The Navy "staffs" for them. No matter what you call it or where you put it, much of that "drudgery" has to be done. The Chief, S5 took some jibes in the form of the assertion that the only reason for the new Office was to improve, on paper, our line-staff ratio. The truth was that, quite apart from the auditor's observations, [redacted] The seven individuals in S5 and S2 most responsible got Presidential citations under a program recognizing major savings in Government. 28% of the total Government savings getting special recognition that year was the work of our people.

[redacted]

~~(C)~~ Now, DDC had five offices, four staffs, and these major projects all demanded managerial time and attention. So, in part to reduce a growing problem of span of control, a new office (S7) was formed in 1977 incorporating all but the HAMPER activity into four Special Project Offices (SPO's), each with Division level status. At the same time, the S1 cryptanalytic organization was split out to form the nucleus of another new Office for COMSEC Evaluations (S6) on a systems-wide basis to include cryptosecurity, TEMPEST, TRANSEC, and physical security.

(U) Ultimately (1978) S4 and S7 were merged into a single Office, S8, which brings us up to date.

EO 1.4.(c)

## THREAT IN ASCENDANCY

~~(C)~~ In olden times, most of our programs, whether in equipment development, TEMPEST, or security procedures were driven largely by our view of COMSEC weaknesses – our *vulnerabilities* – more or less independent of judgments made on the ability of an opponent to exploit them. We assumed hostile SIGINT to be at least as good as ours, and used that as a baseline on what might happen to us. If we perceived a weakness, we would first try for a technical solution – like new crypto-equipment. If the state of that art did not permit such a solution, or could do so only at horrendous expense, we'd look for procedural solutions and, those failing, would leave the problem alone.

~~(C) So~~ our priorities were developed more or less in the abstract, in the sense that they related more to what we were able to do technologically or procedurally than to the probabilities that a given weakness would be exploited in a given operating environment. In short, we did not do much differentiation between vulnerabilities which were usually fairly easy to discover, and threats (which were more difficult to prove) – where threats are fairly rigorously defined to mean demonstrated hostile capabilities, intentions, and/or successes against U.S. communications. The accusations of overkill touched on earlier in part stemmed from that approach.

~~(C)~~ The thrust towards gearing our countermeasures to threat rather than theoretical vulnerability was healthy, and driven by a recognition that our resources were both finite and, for the foreseeable future, inadequate to fix everything. In fact, one of the reactions of an outside analyst to our earlier approach was, "These nuts want to secure the world." Some still think so.

(U) After Vietnam, there was a strong consensus in this country that the U.S. would not again commit forces to potential combat beyond show-the-flag and brush fire operations for a decade or more unless some truly vital interest was at stake – like the invasion of our country. There was a correlative view that such an event would almost certainly not arise in that time frame, and we focussed increasingly on detente and economic warfare.

~~(C)~~ These views, in turn, suggested that threats would be directed more towards strategic $C^3$ communications than tactical ones and that, accordingly, our priorities should go to the former. So, what did we do? We made the largest investment in tactical COMSEC systems in our history – VINSON. We went all out in support of TRI–TAC, a tactical "mobile" system with more engineers out of R1 and S assigned to it than the totality of effort in the strategic communications arena. Further, the bulk of this effort was in support of securing voice and data only on short *wire lines* (a few kilometers) radiating from the TRI–TAC switches.

~~(C)~~ How come? I think it was simply a matter of doing what we knew how to do – arrange to secure multiple subscribers on wire in the complex switching arrangement of the TRI–TAC concept. We did not know how to integrate tactical radios within that concept, and so deferred that problem (called Combat Net Radio Interface) while we built our DSVTs, DLEDs, and elaborate electronic protocols to effect end-to-end encryption. We're getting to it now, but the lion's share of the initial effort was devoted to protecting the least vulnerable communications – the ones on short wire lines in the field.

[redacted]

(U) That sounds like a lot, after all. In peace time, though, most of that kind of information is readily and continuously available through other means – notably HUMINT gathered through routine physical observation, from agent reports, from our own voluminous open publications. . .

(U) I hasten to add that I'd be the last one to push that argument too far. If we denigrate the need for some COMSEC program each time we can point out an alternative way for the information to be obtained,



EO 1.4.(c)

we can talk ourselves out of business. We do, always, need to be sure that voids in COMSEC do not provide the quickest, most reliable, and risk-free ways to obtain our secrets.

~~(S)~~ Despite this major aberration—failure to use threat to determine priority—in the general case, the record has been good. As noted, it was certainly the driving force behind the HAMPER program. It accelerated our work in telemetry encryption. It may hasten the modification or abandonment of some marginally secure systems. It certainly precipitated major improvements in some of our systems and procedures for strategic command and control. In its first real application, it changed an unmanagably ambitious TEMPEST program into one that geared suppression criteria to physical environments and information sensitivity in information processors. And it has shaken loose a variety of efforts to improve physical and transmission security.

(U) A caveat: While nothing gets a user's attention like documented proof that communications *he* thinks are sensitive are being read by an opponent, several things should be borne in mind before telling him about it. Foremost is the fragility of the source of the information (the "proof") you have. Secondly, it is worse than useless to go out and impress a user with a problem unless you have a realistic solution in hand. No matter how dramatic the evidence of threat, if we simply go out and say, "Stop using your black telephone," it's likely to be effective for about two weeks. Don't jeopardize a good source for that kind of payoff.

~~(C)~~ Finally, the results of our own monitoring and analysis of communications, at best, prove vulnerability, not threat, and are often remarkably ineffective. Nothing brought this home more persuasively than the Vietnam experience. Monitoring elements of all four Services demonstrated the vulnerability of tactical voice communications again and again. This did not show that the NVA or VC could do it. It was first argued that they weren't engaged in COMINT at all. Next, that even if they were able to intercept us, they couldn't understand us, especially given our arcane tactical communications jargon. Third, even given interception and comprehension, they could not react in time to use the information.

~~(C-CCO)~~ It took years to dispel those notions with a series of proofs in the form of captured documents, results of prisoner and defector interrogations, some US COMINT and, finally, the capture of an entire enemy COMINT unit: radios, intercept operators, linguists, political cadre and all. Their captured logs showed transcriptions of thousands of US tactical voice communications with evidence that their operators were able to break our troops' home-made point-of-origin, thrust line, and shackle codes *in real time.* The interrogations confirmed their use of tip-off networks (by wire line or courier) to warn their commanders of what we were about to do – where, when, and with what force.

(U) Lamentably, even with that kind of proof, the situation didn't improve much because our "solution" was NESTOR: users did not like that equipment, and they *had* to communicate, anyhow.

## LPI

(U) A traditional way to enhance the security of a transmission is to make it difficult to intercept. The options range from whispering (or the radio equivalent, use of minimum power) to the use of cryptography to spread the transmitted signal unpredictably over a large swatch of the frequency spectrum. In between are armed couriers, physically or electronically protected distribution systems (wire line and, lately, fibre optics), high directivity narrow beam communications (directional antennae and lasers), and hopping randomly and rapidly from one frequency to another.

~~(C)~~ The impetus for the upsurge of interest in LPI (low probability of intercept) radio transmission systems has come not so much from their potential to *secure* communications as from the need to prevent jamming. In other words, it's more a question of communications reliability – assuring delivery – than communications security. As noted in Volume I, this fact raises interesting questions on roles and missions for us – anti-jam being traditionally an EW (electronic warfare) matter, not COMSEC, so why were we "intruding" in this arena? The community seems now to accept the idea that we should (we say "must") participate if cryptographic techniques are employed to lower intercept probability. Thus, while we may provide the key generator to spread or hop a signal, we don't get involved in non-cryptographic anti-jam techniques like the design of directional antenna or brute force very high power transmitters to assure message delivery.

(U) While a primary function of LPI is to prevent jamming, a second one of great importance is to provide protection against an opponent's use of DF (direction finding) to locate mobile military platforms when they transmit. If he can't hear a transmission, he has no way of determining where it came from.

~~(S-NF)~~ Much heavier anti-jam emphasis has arisen because of several developments. First, in the last decade, the focus on Command and Control and the criticality of those communications used to direct forces has intensified, with a recognition that we would be enormously handicapped if those communications were denied to us. The second reason for emphasis stems from growing evidence of Soviet doctrine and supporting capabilities to use EW as a major element of their military tactics and strategy. Finally, some of our forces – notably the Air Force – having begun exercising in "hostile" EW environments, found their capabilities significantly degraded, and thus confirmed a very high vulnerability.

~~(S)~~ In fact, we were stunned when an Air Force study in the European tactical air environment suggested that their vulnerabilities to jamming were greater than those stemming from plain language air-to-air and air-to-ground voice communications. From this CGTAC reportedly concluded that, since they might not be able to afford both COMSEC and anti-jam systems, they would opt for the latter. One senior Air Force officer reportedly said he needed an anti-jam capability so badly he would trade aircraft for it. With a lot of backing and filling, and more extensive study, we helped persuade the Air Force that they really needed both anti-jam and COMSEC. Army had clearly come to that conclusion as early as 1974 when specifications for their new tactical single channel radio (SINCGARS) called for both a COMSEC module and an anti-jam module. The Army, of course, was also the first to get serious about the business of implementing daily changing call signs and frequencies. I believe their and our motivation in pushing for these procedures was to provide defenses against conventional traffic analytic attacks to determine OB (order of battle). But there is an anti-jam advantage as well – by hiding a unit's identity (callsign change) and his location in the spectrum (frequency change), you force the jammer into broadsides – a mindless barrage, not a surgical strike against the specific outfits that worry him most. That, in turn, exposes the jammer himself to hazard – our location of this interfering signal and, perhaps, launching of homing weapons or something else against him.

~~(C)~~ One of the more insidious arguments we faced in some circles where anti-jam was asserted to be more important than COMSEC arose from the fact that ordinary cryptography does not add to the resistance of a transmission to jamming. If you can jam the clear signal, you can jam it in the cipher mode. Further, a smart jammer can work against most encrypted signals more efficiently than against plain text, use less power and be on the air for much briefer intervals. This is true, because all the jammer need do is knock the cryptographic transmitters and receivers out of sync or disrupt the initialization sequences that prefix most encrypted traffic. This is not the case where we employ CTAK (cipher text auto-key) or where synchronization is dependent on internal clocks rather than timing elements of the cipher text itself. All the others are vulnerable if the jammer can stop them from getting into sync in the first place by repeatedly attacking preambles.

## SARK—SOME CAUTIONARY HISTORY

~~(C)~~ SAVILLE *Automatic* Remote Keying (SARK), now usually referred to merely as "Remote Keying," is a subject of mild controversy among the elders as to its origins and original goals. One school of thought (memory) insists it was conceived to solve the logistics problem attendent on continual physical distribution and re-distribution of individual hard copy keys to every holder in every net, with the fall-out benefit of reducing security problems by having fewer copies of compromise-prone keys in the pipe-line, in storage, or in operating locations. The other school recalls just the opposite – an initial drive to find a technical solution to the growing problem of key list compromise – particularly through subversion of cleared individuals – and the logistics benefits a matter of serendipity.

~~(C)~~ Either way, remote keying was the biggest conceptual breakthrough in ways to set up crypto-equipments since the days of the card-reader. But both these potential benefits may be in some jeopardy.

~~(C)~~ VINSON, the prototype vehicle for remote keying, gets its rekeying variable (its "unique" key) from one of three sources: direct from a key variable generator (the KVG) usually held at net control, or from an electronic transfer device (ETD) which has been previously loaded from a KVG, *or from a punched key tape* (manufactured by S3) which can be loaded into an ETD with a special tape reader.

~~(C)~~ For a typical, small, tactical radio net (10–20 holders) the idea was that each subscriber would either go to net control and have his equipment loaded with his variables, or net control would dispatch a courier with an ETD to load his variables *in situ*. Thereafter, he would operate independently of any variables except those electronically stored in his machine until his unique rekeying variable required supersession (usually *one month* unless compromise required sooner change). Meanwhile, he would be rekeyed remotely and independently of any key except that in his machine. No ETD's, no tapes, no couriers, no material to protect except for the keyed machine itself.

~~(C)~~ Despite repeated demonstrations that the concept would work during OPEVAL (operational evaluation) and in a number of nets in Europe where VINSONs were first implemented, it has not, at least so far, worked out that way.

~~(C)~~ We have evidently so sensitized users to the crucial importance of their key that they fear leaving it in their equipments when they are not actually in use. We have conditioned them with forty years of doctrine calling for key removal and safe storage when the equipment is not attended or under direct guard. As a natural consequence, it was an easy step to zeroize equipments at night, hold key tapes or loaded ETD's, and rekey themselves in the morning. Result? Easily recovered key at most user locations, now in the form of key tapes and loaded ETD's – a substitution of one kind of readily recoverable key for another, and our physical security is not much improved over what we had with conventionally keyed systems like NESTOR and the KW-7.

~~(C)~~ Within the next few years, we expect about 140,000 equipments which can be remotely keyed to come into the inventory. At the same time, the users have ordered about 46,000 ETD's and we project the need for 10's of thousands of rolls of key tape to support them, each containing a month's settings. So we're seeing a ratio of *1* to 3 build up, instead of *1* : 10 or less as we had hoped; and our goal of making keys inaccessible to almost everybody in the system may not be realized through remote keying.

THIS PAGE IS INTENTIONALLY BLANK

## THE CRYPTO-IGNITION KEY

[redacted]

P.L. 86-36

THIS PAGE IS INTENTIONALLY BLANK

EO 1.4.(c)

## PCSM

~~(C)~~ One of our most intractable problems has been to find ways to package crypto-equipment in a way which will seriously deter penetration by a smart, well-equipped opponent with plenty of time. The difficulty is not much different than is faced in the manufacture of three-combination safes. The best we can generally afford can stand up to a covert penetration effort by an expert only for 30 minutes or so, and brute force attacks, leaving evidence, can be done much more quickly than that. Yet, these safes are massive and expensive. With a crypto-box, there are added difficulties in protecting logic or resident key because X-ray devices or electronic probing may recover the information without physical entry.

[redacted]

~~(C)~~ For many years we have known that technologies do exist for building protective cocoons around objects that can in fact provide a very high level of resistance to tampering without triggering some alarm. When we first encountered them, we rejected them out of hand as a practical solution to our problem because these "protective membranes" as they were called, could cost on the order of $50,000, each.

~~(S-NF)~~ But more than fifteen years have passed since our first encounter with the technique. The process has been refined, and it now appears that we *might* be able to get such packages for under $500 apiece if we buy in large quantities. This prospect merged in the mind of J. Richard Chiles with the potential for using micro-processors to program various crypto-logics and ancillary functions in a given box. Thus the concept of PCSM – the Programmable COMSEC module – was born.

~~(S-NF)~~ The grand design was (and is) elegant. Encapsulate a micro-computer in a protective membrane. Program it with whatever crypto-logic and assorted keys are required to operate in a given net. Build into each box a unique element of logic or key so that if the membrane is defeated and the contents lost, it will affect no other subscriber's traffic. The membrane serves one function only – to provide, with high confidence, a *penalty* if penetrated. The penalty could range from (theoretically) an explosion to an alarm at some remote place. It might simply zap critical circuitry, disabling the machine, or obliterate all sensitive data (if we learn how to do that).

~~(S-NF)~~ Depending upon the kinds of penalties that prove practical to impose, it may be possible for the entire keyed programmed operational box to be *unclassified*, getting no protection at all beyond that which it provides for itself. Your safe, after all, is not classified. Only its contents. And if all its contents evaporated if somebody (anybody, including you) were to open it, there'd still be no problem. Alternatively, and perhaps more feasibly, it might operate like a bank vault. The money doesn't disappear when somebody breaks in, but other things (alarms) are likely to happen to prevent him from making off with it.

~~(S-NF)~~ A final element in the concept is the use of some central office, switch, net-controller, NSA (!) or some such to electronically check the presence and health of each box. Thus, equipments in storage or in operational locations could not be removed, physically intact without detection, and internal malfunctions in the protective system could be determined without local effort.

~~(C)~~ The goal is not a "perfectly" secure system – rather one good enough to make the risk of detection to an opponent unacceptably high.

~~(S-NF)~~ Maybe by the time somebody writes Volume III of this work, PCSM can be discussed in the present tense. I hope so, because it constitutes the biggest conceptual step forward since remote keying. Most of this material is classified SECRET to help us achieve technological surprise, and it should *not* be discussed outside NSA without prior approval from DDC.

## NET SIZE

~~(C) The~~ cryptosecurity implications of very high volumes of traffic using the same key have not been a dominant factor in determining net size in most of our cryptomachines for many years. Rather, we have opposed very large networks sharing the same key in recognition of the fact that the likelihood of physical compromise rises with the number of copies of materials we make and the number of people to whom it is exposed. Correlatively, the longer a given item is in existence the more opportunities for its compromise arise, and supersession rates are based, in part, on that fact. (A physical security Vulnerability Model has been devised which permits some trade-offs between these two facts – larger nets with more rapid supersession rates, and vice versa.)

~~(C) In~~ olden times, there were limitations on the basic sizes of many communications nets themselves and this put natural limits on shared keying materials when these nets were secured. Now, world-wide compatible communications capabilities are much more prevalent, and operational demands call for more very widely held keys for use in these networks. Eventually, however, there is a sticking point where the risk of compromise becomes prohibitive.

~~(C-NF)~~ Although we've never had any hard statistical probability in our hip pockets, we have generally felt comfortable with net sizes on the order of 250–400 holders, but have tolerated a few nets with upwards of 2000 holders, one KW-7 system with 4900 keys, and the horrendous KI-1A net of 5,945 copies. The rationales for accepting some of the larger nets are sometimes tortured. Instead of looking only at some rough probability of compromise as a function of exposure, we look also at the environment of use – systems in confined enclaves on shipboard seem less vulnerable to compromise than in large plants with many people milling about, or in small field locations where secure structures may not be available. Some systems can be subjected to special protective measures – notably two-man controlled materials – that may offset the existence of large copy counts.

~~(C) The~~ sensitivity or importance of the traffic in given networks may vary greatly, thus affecting the motivations for hostile elements to risk acquiring key, and the long-term security impact should compromise in fact occur. Finally, of course, traffic perishability affects our judgments. In the classic case of KI-1A, we could not care less about the compromise of the key to the world at large one minute after the key is superseded. (This system for identification of friend or foe is useful to any enemy only if he can acquire it before or while it is being used so that he can equip his forces with a means to be taken for a friend.)

~~(S-NF) Still~~ and all, the subjectivity inherent in this approach – as in most physical security judgments – drives us nuts. We are being asked to "quantify" the unquantifiable – the integrity of our people; the physical security conditions at more than 3000 separate cryptographic accounts and the tens or hundreds of individual locations they each may serve; the "value" of tens of millions of messages; the opportunities for subversion, catastrophe, carelessness to result in the compromise of some number of the millions of items we issue annually – and so on. The real force behind the persistent efforts to find technological, measurable solutions to the problems of physical security stems in part from that frustration. There is a justifiable disillusion with our "doctrinal" and "procedural" remedies because enforcement is difficult, they are easy to circumvent deliberately or accidentally by friends and enemies alike, and there is no real way to determine their effectiveness. We *need* the technical solutions – secure packaging, remote keying, PCSM, emergency destruction capabilities, and so on.

~~(S)~~ Meanwhile, let us not rationalize ourselves into some fool's paradise because we have such good and stringent rules and some soothing perceptions that the Soviets, say, aren't really all that proficient. Some of what we still hear today in our own circles when rigorous technical standards are whittled down in the interest of money and time are frighteningly reminiscent of the arrogant Third Reich with their Enigma cryptomachine.

THIS PAGE IS INTENTIONALLY BLANK

## EQUIPMENT CLASSIFICATION

~~(C)~~ One of the more difficult doctrinal issues in our business relates to the level of protection we require for crypto-equipments. As briefly noted in the first Volume, the problem has been around for a long time. By 1970, the pressures for easing our protective criteria had become very strong. Users sought relaxed standards not only on the matter of equipment classification, but also for the whole range of rules regarding clearances, storage, guarding, accounting, access authorization, high risk deployment, key supersession rate, net size, foreign access, and compromise reporting.

~~(C)~~ A special working group was set up consisting of some of our people and representatives of the Services and a few Civil Agencies to review the matter. They found not less than 55 different sets of regulations governing various aspects of the protection of cryptomaterial including basic NSA documents and a myriad of user implementers and amplifiers of those rules. Some contradiction was inevitable. They proposed the elimination of a number of control requirements and drafted a sweeping new, simplified National Level document (NACSI 4005) which emphasized keying material protection, eased the requirements for equipment protection, and allowed classification alone to govern the protection of all other cryptomaterials (maintenance manuals, operating instructions, and so on).

(U) Central to this new departure was the concept of unclassified "Controlled COMSEC Items" (CCI), and the vision that some crypto-equipment, notably tactical equipment, could be, at NSA's discretion, unclassified (but Controlled) when unkeyed.

~~(C)~~ For the record, the background on the whole question is somewhat as follows: Since the mid-50's, various customers had been calling for unclassified equipments, particularly in the tactical arena, and had been resisted by us for reasons of COMSEC, SIGINT, and technology transfer. Throughout the '60's, pressure built as more and more systems proliferated to lower echelons, and culminated with the feed-back from Vietnam about non-use of NESTOR.

~~(C)~~ The two major reasons for declassification were the "inhibition of use" argument, and the vision of full integration of COMSEC circuitry into radios of the future – full integration being defined as inseparable and shared radio and crypto-circuitry. In that configuration, our COMSEC tail would be wagging the communications system dog with the controls classification denotes – how would such equipments be shipped, stored, and particularly, how would they be maintained? "Integration" has thus far not turned out to be the wave of the future. COMSEC modules will by and large be separable from their associated radios because the designers found it more efficient to do it that way. At this writing, only BANCROFT fully embodies the original fully integrated concept. Difficulties in protection will persist even with partial "integration," of course. At the moment, though, they don't look to be nearly as severe as we first perceived.

[redacted]

P.L. 86-36

~~(S-NF)~~ There were seven subsidiary arguments against classification and counter-arguments for each:

• The design assumption of equipment (or logic) loss, countered by facts that such loss is not certain, not necessarily early after design or deployment, and not universal – loss to one or two countries does not equate to loss to all (on the order of 160) others.

[redacted]

• The CONFIDENTIAL clearance offers a low confidence in the integrity of an individual because the investigation is superficial, so what are we really buying in the way of protection? The counter: we are buying a powerful legal sanction against deliberate compromise of the system to an enemy. Lack of classification has been construed as a "near absolute defense" against prosecution – espionage laws, in practice, apply only to classified (and Formerly Restricted Data) information.

• Executive Orders setting up the classification system are awkward when applied literally to hardware – the classification system was clearly designed with two-dimensional objects (paper) principally in mind. Counter: we've nonetheless lived with it rather well. Further, the Executive Order really leaves no option: if loss of the material is judged damaging, it must be classified.

• Dollars for manpower and facilities required to protect classified hardware could be saved. Counter: Savings would not be significant given the requirement for a reasonable alternate set of controls on the equipment – particularly since *classified* keys are used in association with the equipment in operational environments.

• The design of modern equipments can provide inherent protection against logic recovery. Counters: "Secure" or tamper-resistant packaging have not panned out yet. (But see article on PCSM potential.) Similarly, early efforts for extraction resistance and automatic zeroizing have proved disappointing. Early hopes that the complexities and minuteness of micro-electronic components would make their "reverse engineering" difficult have been proven unwarranted.

• Alternative controls to classification could be devised which would provide equivalent or better protection. Counter: when we actually fielded early models of VINSON and PARKHILL as unclassified but Controlled COMSEC Items (CCI) for Service tests, the system broke down. Within a few months, we had an astonishing number of gross violations – lost chips and whole equipments; [redacted] demonstrations of equipments – including remote keying procedures – to boy scouts and wives' clubs, and extremely casual handling. We simply could not articulate the requirements to protect these equipments despite the lack of classification. The nearly universal reaction when we fussed was "If their loss is really damaging to U.S. interests, why aren't they classified?" Without exception, in our contacts with Congressional people, we got that same reaction when they were interceding for constituents demanding a share in the market for Design Controlled (but unclassified) Repair Parts (DCRP's). We learned, the hard way, that classification does significantly lower the probability of compromise.

~~(C)~~ Probably among our less judicious moves in seeking alternative controls for tactical crypto-equipment was the notion of treating them "like a rifle" without first researching what that really meant. On the one hand, it did mean a high level of protection *in the field* because rifles were items for which individuals were personally and continually accountable. Most of these same individuals perceived that their lives might well depend on them. But crypto-equipments – at least until secure squad radios come along – are not items of personal issue, and we have by no means yet convinced most users that their lives may depend on these devices even though we think we can prove that is sometimes true.

~~(S)~~ We also found, of course, that controls over small arms in the Services aren't all that great when they aren't in the hands of individual users. The system for distribution and warehousing is evidently quite weak because DoD acknowledges that many thousands of them cannot be found, or are showing up in large quantities in the hands of various other countries, terrorist groups, the criminal element, and the like.



EO 1.4.(c)

Losses of that magnitude in our crypto-equipment inventory would be disastrous, principally because it would put some elements of DDO out of business.

~~(C)~~ So we backed away from treating them like rifles, and toyed with the idea of treating them like radios. We had heard that such "high value" items got good control, and that protection in the field would be roughly equivalent to that expected for crypto-equipment. The argument was that classification was unnecessary because it offered no real security advantage. We approached this proposition cautiously, partly remembering the large number of tactical US radios that eventually formed the backbone of the North Vietnamese and Viet Cong radio nets, and decided to do an empirical test on the relative protection afforded to radios and crypto-boxes in the same field environment.

~~(C)~~ We enlisted the aid of Army and Air Force counter-intelligence personnel under a project called JAB. During a major exercise (REFORGER '74) in Europe where NESTOR and KI-1A equipment was deployed, we dispatched small counter-intelligence Tiger Teams to see how many crypto-equipments and how many radios they could "acquire" in the same environment. By "acquire" we meant 30 or more minutes of unrestricted access – long enough to steal equipment, extract keys, or recover the internal wiring. The results were interesting.

~~(S-NF)~~ In a few weeks, the team deployed against NESTOR-equipped Army units "acquired" dozens of radios, sometimes together with their parent jeeps and other vehicles. But when they tried to get the CONFIDENTIAL NESTOR's, they met suspicion, distrust, and were nearly caught repeatedly. They managed substantial access to only one NESTOR equipment during the entire operation. That equipment was mounted on a jeep in a guarded motor pool. It was night time, and there was a driving snow-storm. The guard was described as concentrating strictly on the business of keeping alive.

[redacted]

~~(C-NF)~~ Inevitably, after success at three consecutive airbases, some crusty old custodian got suspicious and started checking back on their bona fides. The word went out to AF units all over Europe and they barely escaped arrest at their next target. As you might expect, when they debriefed senior AF officials in Europe, the commanders were considerably more exercised over the fact that the team could have flown off with whole airplanes than with the security of the KI-1A.

~~(C)~~ So, in the Army case, we found a substantial difference in protective levels for radios and crypto-equipments; but in the case where radios and crypto-equipments usually were collocated – i.e., on aircraft – there was no real difference.

[redacted]

~~(S)~~ A much safer way for a hostile government to get at these materials is through subversion of cleared people with routine access to them. This has been done a number of times that we know of, sometimes with very serious consequences. With this technique, some American, not a foreign spy, takes all the risks of getting caught. Until he does, he can offer materials repeatedly as in the most recently publicized case of John Boyce – the employee in a cryptocenter at TRW who was reportedly involved in at least a dozen separate transactions involving sale of keying material and photographs of the logic circuits in one of our crypto-equipments. (The case is well-documented in *The Falcon and the Snowman*. Simon Schuster, 1979.)

~~(S-NF)~~ Coping with this kind of problem is, in part, what remote keying, ignition keys, tamper-resistant packaging and, on the horizon, PCSM are about.

~~(C)~~ The narrative above addresses principally the matter of classification as it relates to crypto-equipment. There follows a more generic treatment of what underlies our efforts to protect cryptographic information in



EO 1.4.(c)

general, and offers a perspective on the kinds of information a SIGINT organization finds useful in doing its job.

~~(S)~~ NSA spends tens of millions of dollars and tens of thousands of man-hours trying to discover what Soviet COMSEC is like. Despite all-source research dating back more than 30 years, the incidence of *any* unclassified statements by the Soviets on any aspect of their COMSEC program is so trivial as to be virtually non-existent. In other words, the Soviets protect (classify) all information about their cryptography and associated communications security measures.

~~(C)~~ The effect of this stone wall has been either to greatly delay U.S. ability to exploit some Soviet communications or to frustrate it altogether.

~~(C)~~ Viewed as an element of economic warfare, we are losing hands down as we expend enormous resources to acquire the same kind of information from the Soviets that we give them free – i.e., without classification.

~~(C)~~ Clearly, the Soviet's classification program costs them something, just as ours costs us. But, they have a cost advantage because they still operate in an essentially closed society with a well-established security infrastructure and with many of their officials already well attuned psychologically to the concept of secrecy.

~~(C)~~ Where we do classify, our tangible costs can be measured in lessened program efficiency and timeliness, and in the cost of the security barriers we then need to build around the information or material. The major intangible penalty is still asserted to be the "net loss" to COMSEC when classification inhibits system use.

~~(S)~~ The optimum attack on any cryptosystem (if you can hack it) is cryptanalytic – you need only operate on cipher text; your risk is low or non-existent unless you have to position yourself dangerously to perform the interception. You don't need to steal keys or penetrate cryptocenters or subvert people and, if you succeed, the return on investment is likely to be rich – all the secrets committed to the cryptosystem in question. [redacted]

~~(S)~~ Accordingly, a first line of defense has to be to protect our cryptologics (and our own diagnoses thereof) for as long as we can, regardless of our sense of the inevitability of eventual compromise. [redacted]

~~(S-CCO)~~ The "SIGINT" argument for protecting our cryptologics is well known – the COMSEC arguments much less so, despite their reiteration for some decades:

- With the exception of true one-time systems, none of our logics is theoretically and provably immune to cryptanalysis – the "approved" ones have simply been shown to adequately resist whatever kinds of crypto-mathematical attacks we, with our finite resources and brains, have been able to think up. We are by no means certain that the Soviet equivalent of A Group can do no better. But no attack is likely to be successful – and certainly cannot be optimized – without preliminary diagnostics – discovery of how it works.
- Systems which have no known cryptanalytic vulnerabilities may still be exploited if, and usually only if, their keying materials have been acquired by the opposition or if their TEMPEST characteristics permit it. In either of these contingencies, however, the logic, the machine itself, or both may be required for exploitation to be successful.

~~(C)~~ Because the thrust for unclassified when unkeyed equipments is lying fallow at the moment, all of the above may seem like beating a dead horse as far as our mainline equipments are concerned. But the matter will assuredly rise again.

~~(C)~~ In any event, most people in S are pretty well sensitized and/or resigned to the need for protecting logics and precise information about their strengths and weaknesses. However, that is not the case with large batches of peripheral information about how we obtain communications system security. We tend to play fast and loose with information about alarm structures, about "TRANSEC" features, depth protection, anti-jam protection, cryptoperiods, keying techniques, testing, financial and logistics arrangements, parts catalogs, plans, schedules, operating instructions, physical safeguards, and usage doctrine in general.

(U) Attempting to protect some of this data is sometimes viewed as hopeless or useless, either because it becomes self-evident the instant a given system hits the street or because it has leaked into the public domain over the years or decades.

~~(C)~~ But beware arguments for declassification on grounds that the information – in bits and pieces – has already been published in unclassified form. Hostile intelligence is not ubiquitous, and we ought not to be compiling "unclassified" data for him, especially when blessed by our rather exceptional stamp of authenticity. And it would be well to remember that our classification of materials on the basis of their aggregate intelligence value still carries weight, despite the discomfiture when people ask which paragraph, which sentence, which word?

(U) But decisions to declassify anything about a new (or old) system should be made case by case, and at least as much thought should go into the whys of declassification as to the whys of classification. I don't think the burden of proof should lie with either the "classifier" or the "declassifier."

(U) In the final analysis, the "classifier" has only two arguments going for him – enhanced security and/or enhanced US SIGINT operations. The "declassifier" likewise has few bottom lines – enhanced COMSEC operations and – often – cost savings. The trouble is, there's usually *some* merit on both sides and, as apples and pears are involved, the "decision" is usually subjective and contentious.

~~(C)~~ The further trouble is the tendency of both "sides" to throw up smokescreens in the form of specious argument or unsupportable assertions – emotionalizing the whole process:

~~(C)~~ COMSEC and SIGINT "classifiers" are quite capable of asserting irreparable harm where little or none exists in the real world – past insistence on patent secrecy for trivial devices being a case in point.

~~(C)~~ Likewise, in the case of the declassifiers – e.g., a tactical voice security advocate claiming the VINSON and PARKHILL programs would collapse if we insisted on their classification.

~~(C-CCO)~~ Perhaps, however, the biggest single shortcoming among people in S deciding on (de)classification of information stems from far too hazy a perception of how the SIGINT world – any SIGINT world – operates, and the practical difficulty that world encounters in acquiring all the data they need to target and exploit a given communication system. The process is expensive and complex, and entails well-defined steps of collection, forwarding, processing, analysis, and reporting.

~~(C)~~ Before committing assets to an attack, they need to know not just the cryptosystem, but the associated communications, the nature of the underlying traffic, deployment plans – where, when, who, how many. So the data that is valuable to them includes:

- The size of the program
  - How much are we spending on it
  - How many copies will we build
- Who the users are
- Where they will be located
- Communications platforms and frequencies
- Deployment schedules, TechEvals, OpEvals, IOC's etc.

~~(S)~~ Given all that, and the cryptologic, they can begin to get down to the serious work of deploying collection assets, adjusting targetting priorities, massing the people and equipment at home or in the field to carry out attack. That may take *years*. Thus, in short, the more advance knowledge of future crypto-system deployments they have, the better they can plan and schedule their attack. Were we ever to field a major cryptosystem with complete surprise (we never have), we might well be home free for some years even if that system had some fatal flaw of which we were unaware.

~~(C-CCO)~~ So, one root question we need to ask ourselves when we are trying to decide whether something need be classified or not is: "What would be the value of the information if I were part of a hostile SIGINT organization – any such organization?" "Will its protection block or delay potential efforts against us?" A correlative question – equally difficult for COMSEC people to answer – is: "will it be useful to an actual or potential US SIGINT target by showing that target something it can use to improve its own COMSEC equipment or procedures?" "What would our own SIGINT people give for comparable information about targetted foreign cryptography?" A trap to avoid in attempting that answer is conjuring up only the Soviet Union as the "target" in question. Clearly, there are categories of information which would be of little use to them because of the level of sophistication they have already achieved in their own cryptography, but could be of extreme value to other countries.

[redacted]

~~(C)~~ All this activity culminated in our abandoment, at least for now, of the commitment to make most tactical equipment unclassified. Our announcement to that effect caused some grumbling among our customers, but not the brouhaha we had anticipated.

EO 1.4.(c)

## PUBLIC CRYPTOGRAPHY—SOME CAUSES & CONSEQUENCES

(U) This strange term remains imperfectly defined at this writing. It seems to relate to all of the following:

- Commercially designed cryptosystems available to the general public.
- Government-designed (or endorsed) cryptosystems made similarly available.
- Cryptographic schemes and cryptanalytic treatises published in open literature by academicians and others interested in the subject.

~~(S)~~ While commercial equipment has been around for many decades, their quantity and variety was relatively small. Most were manufactured overseas – particularly in Switzerland, and no huge market existed for them after World War II because many Governments (like our own) began increasingly to use systems exclusively of their own design and under their own control. Similarly, the amount of published literature on cryptography, and particularly on sophisticated cryptanalytic ideas was sparse. In the U.S., the Government (specifically, NSA) enjoyed a near-monopoly on the subject by the early '50's. That persisted until about 1970, when a dramatic change occurred.

~~(S)~~ A handful of U.S. companies interested in computers, in communications, or in electronics began to perceive a market for electronic crypto-equipments. A few other American companies began building crypto-equipment in competition with the Swiss and others in Europe, supplying devices to some Governments in Africa, South America, and the Middle East and to a few major corporations – notably some oil companies seeking to protect vital industrial secrets.

(U) At about the same time, the question of computer security, which had been on the back burner since the late 50's, began to get a great deal of attention from computer manufacturers themselves and from some of their customers. Computer fraud had become more common, and its impact, particularly on the banking world, became significant.

(U) In 1974, the Privacy Act (P.L. 93–539) was passed, imposing a legal obligation on Government Departments and Agencies to protect the information held on private citizens – notably in computer banks. Since data was increasingly being communicated among computers, the need for some means to secure these transmissions became evident. Thus, the perception of a need for encryption arose in the public sector.

(U) The Department of Commerce has an element charged with improving the utilization and management of computers and ADP systems in the Government. They, especially, perceived a requirement for commercial sources for cryptography to protect Government computer communications and, correlatively, the need for an Encryption Standard applicable to any system offered to Government against which commercial vendors could design security devices. This Standard, the Data Encryption Standard (DES), was published by the National Bureau of Standards as Federal Information Processing Standard No. 46 in January, 1977.

(U) The process involved solicitation for proposals for such a "standard" encryption process or algorithm and two public symposia were held by NBS to discuss the merits of the winning submission (IBM's). A small storm of controversy erupted when some academicians said it wasn't good enough, and implied it had been deliberately weakened so that the Government could break it. Heretofore, in the COMSEC business, publicity of any kind – much less adverse publicity – was rare, and we were not happy. However, a Congressional investigation exonerated NSA and the issue subsided somewhat.



EO 1.4.(c)

[redacted]

~~(C)~~ By this time, we had bitten the bullet, deciding to seek a generic COMSEC solution. This was a decision of enormous consequence for us. The notion of injecting Communications Security into the commercial world in a big way was unprecedented, with serious policy, political, and technical implications for all involved. Principal players became ourselves, the telephone companies, the White House, DCA, the now defunct Office of Telecommunications Policy in OMB, FCC and, ultimately many users of the commerical telephone system.

[redacted]

~~(C)~~ The doctrinal problems were large and intractable because they involved the provision of cryptography in unclassified environments where many of our traditional physical security measures were thought to be inapplicable. How would the crypto-equipments be protected? How to protect the keys? How do you effect key distribution with no secure delivery infrastructure such as we enjoy in the Government COMSEC world? Problems of this kind led to a campaign to use the DES – the only unclassified Government-approved cryptosystem available, thus solving the physical security problem insofar as the crypto-equipment itself was concerned. The root difficulty with this proposal from the security analysts' viewpoint lay in the fact that the DES algorithm was originally designed and endorsed exclusively for the protection of unclassified data, fundamentally to insure privacy, and without a SIGINT adversary with the power of the Soviet Union having been postulated as a likely attacker. Accordingly, the system was not designed to meet our high grade standards and we were not interested in educating the world at large in the best we can do.

~~(S)~~ Nonetheless, the system is very strong; has stood up to our continuing analysis, and we still see no solution to it short of a brute force exhaustion of all its $2^{56}$ variables. It is good enough, in fact, to have caused our Director to endorse it not only for its original computer privacy purposes, but for selected classified traffic as well. Cynics, however, still ask "Are we breaking it?" The answer is no. But could we? The answer is "I don't know; if I did I wouldn't tell you." And there's a good reason for this diffidence. A "No" answer sets an upper limit on our analytic power. A "Yes" answer, a lower limit. Both of those limits are important secrets because of the insights the information would provide to opponents on the security of their own systems.

~~(C)~~ The event with the most far-reaching consequences which stemmed in part from our having grabbed this tiger by the tail was the re-organization of the COMSEC effort at the National level. Historically, NSA had been the *de facto* and *de jure* National Authority for all Government cryptographic matters – a position



EO 1.4.(c)

established by sundry Executive Orders, Directives, "charter" documents and the like reaching back to 1953. But, by mid-1976, attacks on us by a small but vocal contingent of Academe had become bitter. Some elements of the National Science Foundation which underwrote much of the cryptographic work done in the private sector joined in the beginnings of the adversarial relationship vis a vis NSA.

~~(C)~~ A fundamental challenge related to the *propriety* of an "intelligence" organization having jurisdiction over the privacy of citizens in the post-Watergate climate. In short, could we be trusted? An early action of the Carter Administration, therefore, was to issue a Policy Review Memorandum (PRM 21), to examine this issue and recommend a course of action. The result – 11 months later (Nov '77) – was a Presidential Directive (PD 24) effecting a basic realignment of roles and missions in Government for COMSEC and for something different called "Telecommunications Protection."

~~(C)~~ The Secretary of Defense remained the Executive Agent for Communications Security, but with COMSEC now defined to relate only to the protection of classified information and *other information related to national security.* A new Executive Agent, the Secretary of Commerce, became responsible for "Telecommunications Protection," defined to encompass information *not related to national security.* In both cases, the threat was defined to be exclusively "foreign adversaries" and nobody was charged with "domestic" threat – e.g., those engaged in computer fraud, industrial espionage, drug smugglers, terrorists, and the like who may be exploiting communications.

~~(C)~~ So, the split-out of roles and missions did not relate in any direct way to the kind of cryptography or other protective measures that may be used, nor to the specific customers to be served by one Executive Agent or the other, nor to the specific communications means in question nor, finally, to the nature of the opposition. It relates only to the underlying nature of the information to be secured (protected). For the past two years or more, we and the Department of Commerce have been trying to sort it out. Not the least of the difficulties is that many communications systems carry a mix of security-related and non-security related information – notably, of course, those of the telephone companies. So who's in charge?

~~(C)~~ While these events gathered steam, the HAMPER program faltered because of uncertainties on who was charged with, responsible for, authorized to, or capable of moving forward. Big money was involved, and we didn't know who should budget for it. Should the common carriers pay for it themselves, or its customers? Or the government? It is, after all, a security service that most may not want or perceive a need for.

~~(C)~~ A handful of people from the now defunct Office of Telecommunications Policy (OTP) were transferred to a new organization within the Department of Commerce (DoC) to form the nucleus of an Agency charged to implement their part of PD–24. The new Agency is called the National Telecommunications and Information Agency (NTIA) and they are the people with whom we deal daily in trying to carry out our obviously overlapping missions. A few of our former colleagues joined that Agency to help them acquire the technical competence to deal with cryptographic questions, system selection, application, and the like. We are travelling a rocky road in these mutual endeavors because, quite apart from the potential for jurisdictional dispute, we have philosophically different orientations. By and large, most people in both the COMSEC and SIGINT organizations in NSA believe that we can accomplish our missions more effectively in considerable secrecy because it helps us to conceal our strengths and weaknesses and to achieve technological surprise. DoC, on the other hand, is in business, in part, to encourage private enterprise, to maximize commercial markets at home and abroad, and to exploit the products of our own Industry for use in Government rather than having the Government compete with Industry – and this does not exclude cryptography.

~~(C)~~ While, in DoD, Technology Transfer is viewed largely as a security issue with concerns oriented towards export control for critical technologies, Commerce is interested in the infusion of our own industry with technologies now controlled by the government. They need, therefore, to maximize the declassification of information relating to cryptography. Their in-house resources remain meager, so they are turning to commercial research organizations to develop cryptographic expertise. Since these contracts are usually unclassified, and we fear the consequences of publications of what the best private sector brains may have to offer, there is some continuing tension between us.

~~(C)~~ Through all this controversy, and notwithstanding our security concerns (some will read "paranoia"), there is a very strong motivation among us for cooperation with DoC, with Industry, and with the Academic community to get the Government's business done. Clearly, because of that near-monopoly I spoke of, we have a head start in NSA on cryptographic matters. Just as clearly, we have no monopoly on brains nor on manufacturing innovation and ingenuity. Potential security losses may well be off-set by what a motivated commercial world and interested Academe might offer to the Government for its own use. There is a school of thought that believes that various commercial offerings – notably those which may embody the DES – may fill a gap in our cryptographic inventory which our own systems cannot fill because of their design against high and costly standards and tough military specifications, their protection requirements, and the protracted periods of time they generally take to produce. Note, for example, that after all these years, a significant majority of military voice communications and almost all non-military Governmental voice communications remain unsecured. Inexpensive and quickly available commercial voice equipments might move into this vacuum and – even though they may generally offer less security – we might enjoy a net gain because otherwise, for many years to come, those communications will be there for the taking, essentially free of cost to an opponent. This argument does not mollify the conservative, however.

(U) At this writing, some uncertainty remains as to how large the market for commercial devices, notably DES, may be. There seems to be a consensus that they may be applied in considerable quantity to protect or authenticate the contents of messages in support of financial transactions, and most especially in the field called Electronics Fund Transfer (EFT) because of demonstrated vulnerability to costly fraud.

(U) But, although a Government endorsed technique has now been on the street for a number of years, there has as yet been no rush to acquire equipments in quantity. This may be due, in part, to significantly lower perceptions of threat on the part of prospective customers than projected by ourselves and others. It may also stem, in part, from the slowness with which supporting Government standards and guidelines are being published (for Interoperability, Security Requirements, etc.)

(U) In any event, production and marketing of equipment by U.S. commercial vendors is not our biggest problem with public cryptography because there are various Government controls on such equipment – particularly, export controls – and Industry itself is usually disinterested in publishing the cryptanalytic aspects of their research in any detail. The central issue that continues to fester is encapsulated in the phrase: "Academic Freedom *versus* National Security."

(U) Our Director has made a number of overtures to various academic forums and individuals in an effort to de-fuse this issue, but has stuck to his guns with the statement that unrestrained academic research and publication of results can adversely affect National Security. While a few academicians have been sympathetic, the more usual reaction – at least that reaching the press – has been negative.

~~(C)~~ The principal reason that there is an NSA consensus that unrestrained academic work has a potential for harm to our mission is because, if first-class U.S. mathematicians, computer scientists, and engineers begin to probe deeply into cryptology, and especially into cryptanalytics, they are likely to educate U.S. SIGINT target countries who may react with improved COMSEC. Less likely, but possible, is their potential for discovering and publishing analytic techniques that might put some U.S. cryptosystems in some jeopardy.

(U) The academicians' arguments focus on absolute freedom to research and publish what they please, a rejection of any stifling of intellectual pursuit, and concerns for the chilling effect of any requests for restraint. Their views are bolstered by the real difficulty in differentiating various kinds of mathematical research from "crypto-mathematics" – notably in the burgeoning mathematical field of Computational Complexity, often seeking solutions to difficult computational problems not unlike those posed by good cryptosystems.

~~(C)~~ As a practical matter, Government "leverage," if any, is rather limited. We have made some half-hearted attempts to draw an analogy between our concerns for cryptology with those for private research and development in the nuclear weapons field which led to the Atomic Energy Act that does – at least in theory – constrain open work in that field. But there is no comparable public perception of clear and present danger in the case of cryptology and, despite the "law," academicians have sanctioned research revelatory of atomic secrets including publications on how to build an atomic bomb.

~~(C)~~ Another wedge, which as yet has not been driven with any appreciable force, is the fact that – overwhelmingly – the money underwriting serious unclassified academic research in cryptography comes from the Government itself. Among them are the National Science Foundation (NSF), the Office of Naval

Research (ONR) and the Defense Advanced Research Projects Agency (DARPA). NSA supplies a little itself. The wedge is blunted because Government officials administering grants from most of these institutuions have been drawn largely from the academic community who believe strongly in the value of research performed outside Government, and are sympathetic to concerns about abridgement of Academic Freedom.

~~(C)~~ In the long run, balancing out our mutual concerns will probably depend more on the good will of influential sections of the Academic Community itself than on legislative, monetary or other control over cryptographic research in the private sector. It turns out that at least some governing bodies in various colleges and universities seem more ready to recognize some academic responsibility with respect to national security concerns than do many individual "young Turk" professors or their collective spokesmen who see Academic Freedom in First Amendment terms as an absolute. A good deal of the Director's quiet work on the matter appears to be oriented towards constructive dialog with responsible officials and groups.

~~(S)~~ I have dwelt on the matter of public cryptography at some length because it portends some radical changes in our relationship with the public sector – more openness, dialog, controversy, and debate. Obviously, our conventional shield of secrecy is undergoing some perforation. In contrast, it might be worth noting that we have yet to see a single unclassified document from the USSR on their cryptography – not one word. (As a result, we spend small fortunes acquiring data comparable to that which realities suggest we must continue to cough up for free.)

(U) Nonetheless, I believe we can identify and continue to protect our most vital interests – our "core secrets" – and, meanwhile, dialog with intelligent people – even "opponents" – will surely expand our own knowledge and perspective.

~~(C)~~ A more tangible outgrowth of public cryptography could be the infusion of commercial equipment in Government for the first time since World War II. As noted earlier, the votes are not yet in on how prevelant that may be; but it bodes new sets of problems in standards, doctrine, maintenance, protection, configuration control, cost benefit analyses, and secrecy

(U) How do we offer a reasonable COMSEC education to U.S. users in unclassified environments without educating the world?

~~(C)~~ How do we underwrite, endorse, certify, approve or otherwise sanction products in the abstract when their real security potential may well lie in how they are applied in a systems complex, not just on a good algorithm? Or how, alternatively, do we find the resources required to assess dozens of different devices in hundreds of different applications?

(U) We are currently wrestling with all these questions; but most of them will be incompletely answered for a long time. It may be useful for you to keep them in mind as you get involved with public cryptography downstream.

EO 1.4.(c)

THIS PAGE IS INTENTIONALLY BLANK

EO 1.4.(d)

## PKC

~~(C)~~ One of the more interesting outgrowths of the burgeoning interest in cryptography in the private sector was the "invention" of a concept called "Public Key Cryptography" (PKC). All conventional cryptography requires the pre-positioning of shared keys with each communicant. The logistics for the manufacturing and delivery of those keys keeps S3 in business and forces users to maintain a large secure crypto-distribution system. (Remote keying eases but does not eliminate the problem.) The thought was, cryptography would be revolutionized if a system could be devised in which people could communicate securely without prior exchange of keys.

(U) The main idea that came forward was an effort to capitalize on the fact that some mathematical functions are easy to carry out in one "direction," but difficult or impossible to reverse. A classic example of these so-called one-way functions is the phenomenon that it is not hard to multiply two very large prime numbers together, but given only their product, no elegant way has been put forward for determining what the two original numbers were.

(U) So the original numbers could be considered to be part of one man's secret "key:" their product could be published; an encryption algorithm could be specified operating on that product which could not be efficiently decrypted without knowledge of the "key"; and all messages addressed to that person would be encrypted by that algorithm.

[redacted]

(U) It was an interesting mathematical puzzle, first put forward centuries ago, but with no great incentives for its solution beyond the satisfaction of intellectual curiosity, no perceived commercial applications, and so on. So there was no evidence of a great many brains having worked the problem over the years; nor did we go all out against it because, apart from theoretical doubts, there were other drawbacks.

~~(C)~~ The most obvious – although perhaps not the most important – was the fact that the encrypter himself could never decrypt his own message – he would be using the cryptosystem of the recipient who was the only one holding the secret decrypting key – he would have no means to verify its accuracy or correct an error. More or less elaborate protocols involving hand-shaking between the communications were put forward to get around this difficulty – usually entailing the receiver having to re-encrypt the received message in the sender's key and asking if that was right. A clumsy business.

~~(C)~~ Next, each user would have to keep his primes absolutely secret, forcing on each some of the secure storage and control problems inherent within conventional schemes. Known (or unknown) loss would compromise all of his previously received messages. To get around that, relatively frequent change would be necessary. This would move him towards the conventions of keying material supersession; generation and selection of suitable primes and their products, and their republication to all potential correspondents.

~~(C)~~ Next was the matter of efficiency. The "key" would have to be on the order of 1000 bits long to make factorization difficult (or impossible?). Inherent in the scheme is the requirement to use all of that key for any message, however short. Further, a single garble renders the entire message unintelligible.

(U) In the more detailed schemes outlined so far, generation and manipulation of very large numbers is required, including raising them to some as yet undetermined power – but clearly more than just squaring them – and this leads to great complexity in any real implementation of the idea.

~~(C)~~ Finally, there is the problem of spoofability. Anyone can send you a message in your key which you must either accept as valid or authenticate somehow. If I inject myself in your communications path, I may purport to be anybody, supply you my key, shake hands like a legitimate originator and lead you down various garden paths indefinitely.

~~(C)~~ So we are not yet prepared to accept PKC as a wave of the future. However, it continues to offer intriguing possibilities, particularly for short messages resupplying conventional keys among small user sets, and we may eventually find some use for it if we can do so without creating problems at least equal to those it is designed to solve.

## COMPUTER CRYPTOGRAPHY

~~(S)~~ Since most crypto-equipments these days can be viewed essentially as hard-wired special purpose computers with "programmable features" to accommodate variables, there has been considerable effort, dating at least to the early '60's, to use general purpose (GP) computers to do cryptographic functions – programming the whole process, encryption algorithm and all. The idea was particularly attractive at installations where some GP computer with excess capacity was already in place. The first operational system I recall was used to decrypt telemetry from the Navy's first position location satellite – the Transit system, in a shipboard computer, the BRN-3, implemented in 1963. Since the computer was required anyhow to carry out navigational calculations based on data received from the satellite, since it operated in a receive only mode (the sender was a conventional black box in the satellite), and since operation was "system high" (i.e., all personnel with access to any part of the computer were fully cleared for all the data being processed), no big computer security problems were involved – rather, it was a technical matter of programming cryptography efficiently into a system not originally designed to carry out such functions.

~~(C)~~ Nevertheless, there has been little proliferation of computer cryptography in the ensuing years, mainly because the inherent constraints in the BRN-3 environment (excess capacity, system high operation, receive mode only, and rigorous access control) are still not prevalent. The security problems that arise when one or more of those limits disappear are difficult indeed. If, as is increasingly the case these days, the computer can be remotely accessed by various subscribers, the difficulty is greatly compounded. This is true because the vulnerability of sensitive data in a computer to inadvertent or deliberate access, extraction, pindown, disruption, tampering, misrouting, or other manipulation increases as you increase the opportunities for physical or electronic access to it. In this respect, the problem of insuring the security integrity of cryptographic information in a computer is no different than with "computer security" in general. As you no doubt know, that general problem is being assaulted on many fronts today with efforts to make "provably secure" operating systems, the development of the "security kernel" concept, kernelized virtual machines and so on. The threats are so numerous that a 247 page document ("ADP Security Design and Operating Standards", by Ryan Page) is still not definitive.

~~(C)~~ Not the least of our worries with computer encryption proposals is the question of how to evaluate their security potential, how to validate large software programs such as you would need to implement, say, SAVILLE in software; and how to insure that "peripheral" changes elsewhere in the computer will not affect the integrity of the cryptography. It turns out, naturally enough, that S6 proceeds with diminishing confidence as systems become more complex, and with more and more functions not under the cryptographic designer's control which yet may affect the way the cryptography works. Control functions, timing functions, switching functions, etc., are typical examples of these "peripheral" activities that don't remain static – i.e., aren't hard-wired – and subject to change to facilitate other functions in the computer as time goes by.

~~(C)~~ Two other factors have slowed the rush towards computer cryptography. The first is that most commercially available computers still have TEMPEST problems. Few meet our TEMPEST standards for crypto-equipments (KAG-30), and they are difficult to fix. The other factor is that the dedicated (special purpose) computer – an ordinary cipher machine, for example – can always carry out a single job more *efficiently* (space, speed, power consumption, and so on) than one with multiple functions.

(U) None of this means we can't do it – but we aren't there yet. And it's just possible that it's another of those waves of the future that will dissipate in the sea of time.

THIS PAGE IS INTENTIONALLY BLANK

## POSTSCRIPT

[redacted]

(U) Or so it often seems to someone trying to whip up some enthusiasm for a change.

[redacted]

EO 1.4.(c)

THIS PAGE IS INTENTIONALLY BLANK

## TEMPEST UPDATE

~~(C)~~ TEMPEST difficulties seem to whipsaw us more than any of the other technical security problems we have. Each time we seem to have achieved a reasonably well-balanced and managed program in NSA, other Agencies, and in the Industrial TEMPEST Program (ITP), some new class of problems arises. Better detection techniques call some of our older standards into question. New phenomena or variations of old ones are discovered. New kinds of information processors come into the inventory from the commercial world posing different suppression problems. Vulnerabilities remain easier to define than threat in most environments, and we seem to wax hot and cold on how aggressively the whole problem should be attacked.

~~(S-NF)~~ The proliferation of Cathode Ray Tube display consoles (CRT's) is among the more recent examples to catch our attention and that of our customers. Most computers and their peripherals still come off the shelf from Industry without much TEMPEST protection built in. Customers may lay on tests after installation and if they see problems in their particular facilities, may try to screen them or, if threat perception allows, take their chances on hostile exploitation. But with CRT's, two things happened. First, they were more energetic radiators than most other information processors unless TEMPEST suppression (at greater cost) had been applied during manufacture. Second, the results of testing of an insecure device were horribly obvious. Testers, instead of having to show some skeptical administrator a bunch of meaningless pips and squiggles on a visicorder and esoteric charts on signal to noise ratios, attentuation, etc., could confront him with a photocopy of the actual face of his CRT with the displayed data fully legible, and could demonstrate instantaneous (real time) recovery of all of it from hundreds of yards away. This gets their attention.

~~(C)~~ However, as seems to be the case with many of our more dramatic demonstrations of threat or vulnerability, the impact is often short-lived, and the education process soon must start again. But, despite the apparent fluctuations in threat perception and correlative command interest, the resources in R&D and personnel committed to TEMPEST problems in NSA and the Services remains fairly consistent, [redacted]

~~(S)~~ It's fair to conclude that the problem will be with us as long as current flows, but the earlier judgment that we have it reasonably well in hand except in unusually difficult environments may have been too sanguine. We are being faced with more and more types of sophisticated information processors – including computer-based systems – and these are proliferating at a greater rate than we can track. This fact, coupled with more widespread knowledge of the phenomenon, the decline in the availability of trained technical personnel for testing and corrective action in the field (some test schedules have fallen as far as two years behind), and the advent of more potent exploitation devices and techniques place us in a less than satisfactory posture.

P.L. 86-36

THIS PAGE IS INTENTIONALLY BLANK

## SFA REVISITED

~~(C)~~ "SFA" used to stand for "Single Failure Analysis." In the early 70's, a somewhat more elegant but less precise meaning arose – "Security Fault Analysis." It is a systematic process for examining the embodiment of a cryptologic to determine the security effect of malfunction or failure of individual components, switches, circuits, registers, gates and the like. Its purpose is to assure that any fault which would have a catastrophic effect on systems security is safeguarded against – usually through redundancy in design or some kind of alarm.

~~(C)~~ A classic example of catastrophic failure is one which allows plain language being encrypted to by-pass the key generator altogether and be transmitted in the clear. Another – usually more insidious – is a failure in randomizer circuitry causing predictable or repetitive initial set-ups for a machine.

~~(S)~~ SFA had its beginnings with relatively simple electro-mechanical devices where pins might stick, switches hang up, or rotors fail to move, and no truly systemized examination for such failures was carried out or necessary. Most of those failures were not visualized and prevented during design. Rather, when they cropped up in the field and were reported, we would have to go back and retrofit. We had, for example, a case with a duplex one-time tape circuit where an operator noticed that an exact copy of his outgoing traffic was being printed, in the clear, on his receive teletypewriter. He thought a previous operator had jacked that teleprinter in to provide a monitor copy to assure accuracy of his send traffic. What had really happened was a simple failure of a Sigma Relay at the distant end of the circuit which caused the incoming messages, after decryption, to not only print out normally on his receiver but also to be shunted back, in the clear, over his send line. In another case, an on-line rotor system called GORGON seemed to be operating perfectly all day long when an operator noticed that the familiar clunking sound of moving rotors seemed to be missing. He lifted the lid to the rotor basket and discovered why. There were no rotors in it. Ordinarily, that would have caused continuous garble at the distant end, and the operator there would have sent back a BREAK to stop transmission. In this case, however, the distant end had *also* forgotten to put the rotors in, and so received perfect copy in the clear, but believed it to be decrypted text.

~~(C)~~ It worked out alright, though. For their part, the analysts began to get more precise about what constituted a critical failure. The designers meanwhile, through systematization of the process during equipment manufacture, found ways to anticipate problems and avoid some of the back-fitting which had previously been necessary. As is usually the case in our business, when security requirements conflict with cost in time and money, a fairly pragmatic trade-off is made. We have yet to build a machine deemed perfect from the security analysts' viewpoint, and I doubt we ever will. On the other hand, we've made few if any equipments against which security design overkill has not been asserted by its builders or the budget people, or both.

P.L. 86-36

THIS PAGE IS INTENTIONALLY BLANK

## NESTOR IN VIETNAM

~~(S)~~ Most US SIGINT assets in Vietnam used NESTOR heavily and successfully almost from the outset. Towards the end of the war, so did most in-country Naval forces, particularly airborne assets. In the SIGINT user's case, it was because they were already equipped when they got in country; had used it previously, knew, accepted, or circumvented its peculiarities, and, of course, because they believed their traffic required protection. In the Navy case, it was the result of Draconian measures by the Commander, Naval Forces, Vietnam (COMNAVFORV). That Admiral happened to be a COMSEC believer; so he told his pilots that if they didn't use the equipment, he'd ground them. Some didn't, and he did. There is, I understand, no comparable trauma for a fighter pilot.

(U) The story with most of the rest of the "users" was quite different, and very sad. The reasons and excuses were manifold, and a few will be treated here for what might be learned from it.

~~(C)~~ It was claimed that NESTOR reduced radio range. In an environment where communicators were only marginally able to reach one another anyhow, this was intolerable. Experiments at NSA before the equipment was deployed, and repeated investigations when these claims persisted, verified that NESTOR did not reduce range. They even showed that the system could sometimes enhance communications by holding higher voice quality (less noise) towards range limits; although when it reached the limit, loss of all intelligibility was abrupt and categorical.

~~(C)~~ Finally, our own engineers sent to Vietnam reported back: "Sorry about that, S2; the system reduces range – typically by 10% or more." And it, in fact, did. It turned out that NESTOR did not affect range only if the associated radio was perfectly tuned, "peaked," matched to the NESTOR equipment (as we naturally did here at home). In the field, maintenance personnel were neither trained nor equipped for such refinement – the test instrumentation simply did not exist there, and we had not anticipated those real world conditions when we sent it out.

~~(C)~~ In tactical air, it was claimed that the sync delay – up to 3/5 of a second of required wait between pushing to talk and ability to communicate – was intolerable when air-to-air warnings among pilots had to be instantaneous. A survey showed, by the away, that most pilots judged this time to be on the order of three seconds; so, in fact, the wait must have seemed interminable when one wanted to say "Bandit at two o'clock."

~~(C)~~ Carrier-based aircraft ultimately adopted what was called a "feet wet-feet dry" policy in which they would operate exclusively in cipher while over water, but once over land, would revert to plain language. For Air Force pilots, it was not so much of a problem. They managed to install so few equipments in their aircraft, that they were able to create few viable crypto-nets, so most of them were in clear all the time.

~~(C)~~ Navy had managed to jury-rig NESTOR (KY-28) equipment in essentially every carrier-based fighter aircraft they had. In the case of the F4 they found a nook inside the nose-gear housing, and tucked it in there. But the Air Force opted to go into a major aircraft modification program to accommodate the system, penetrating the skin and with elaborate wiring to remote the system to the cockpit. This took *years*. The problem was compounded because when aircraft did get in country with NESTOR's installed, they were periodically recalled to CONUS for maintenance and rehabilitation, took their NESTOR with them as part of the avionics package, and were replaced with unequipped planes.

~~(C)~~ The ground version of NESTOR (KY-8) would not run in high ambient temperature. True. And there was plenty of such temperature around in Vietnam. There was an inelegant but effective solution to that one. The equipments were draped with burlap and periodically wetted down. So much for our high technology.

~~(C)~~ There was a shortage of cables to connect NESTOR to its associated radio. This sounds like a small and easily solvable difficulty; but it turned out to be one of the biggest and most persistent we had. It stemmed from a deeper logistics problem because different organizations were responsible for fielding the various components that went into a secure tactical system. We procured the NESTOR equipment. Various Service organizations procured the various radios with which it was used; and still different organizations fabricated cables and connectors to link them up. Systems planners and implementers in Vietnam eventually gave up and appealed to CINCPAC to orchestrate a coherent program. CINCPAC gave up and appealed to JCS (who may have done a staff study), and it was never solved.

~~(C)~~ Some NESTOR users had AM radios, some FM, and ne'er the twain would meet even though they were cooperating forces.

~~(C)~~ Over the length and breadth of South Vietnam were many cryptographically unique NESTOR nets (i.e., different key lists) to comply with doctrinal rules limiting net size because of the high vulnerablility to compromise of keys in that environment. The limit started out at about 250 holders, was extended to 400, and we eventually tolerated a country-wide net for air-to-air/air-ground communications to accommodate aircraft which might show up anywhere.

~~(C)~~ The manpack version (KY-38) was too heavy - KY-38 plus PRC 77 radio, plus batteries, plus spare batteries weighed about 54 pounds. The Marines, especially, tried to overcome this, even going so far as to experiment with two-man carries, one toting the 38, the other the radio, and with a cable between them. As you might imagine, that worked none too well in the jungle, and I believe most of them decided that carrying ammunition would be more profitable for them.

~~(C)~~ NESTOR is classified, people fear its loss, careers may be in jeopardy, and it was safer to leave it home. This Unicorn - this mythical beast - was the most aggravating, persistent, elusive, and emotional doctrinal issue to come out of that war. We sent emissaries to a hundred locations. We found no qualms about associated keying materials always with the equipment, and which were almost always more highly classified than the equipment itself. We found no concern over keyed CIRCE devices issued in well over 100,000 copies; and we found another CONFIDENTIAL tactical equipment, KW-7, used with enthusiasm as far forward as they could get power. Our records show that the exact number of NESTOR equipments lost as a result of Vietnam was 1001, including a number that were abandoned when we were routed, but mostly in downed fixed wing aircraft and choppers, and in overruns of ground elements. We found no evidence of "disciplinary" action because somebody lost a NESTOR while trying to fight a war with it, nor, in fact, for any other cause. Yet, "classification inhibits use" remains a potent anti-classification argument for all crypto-equipment to this day.

~~(S)~~ The argument in the Vietnam context came as close to being put to rest as I suppose it ever will be by a major [redacted] study published in 1971. By that time the matter of non-use of NESTOR had become a burning issue. Here, an expensive crash program had been undertaken by NSA to build and field 17,000 KY-28's and 38's; a bonus of $3 million had been paid for quick delivery. The total NESTOR inventory exceeds 30,000, yet best estimates in 1970 suggested that only about one in ten of the devices was being used. A questionnaire was administered to about 800 individuals who had had some exposure to the system in SEA. It contained a dozen or so questions, all oriented towards determining why the system was not being used more heavily. Some of the more relevant findings are quoted below:

~~(C)~~ How do you feel that the use of tactical secure voice equipments affects the operations of your unit?

1—Speeds up and improves operations

2—Slows down and interferes with operations

3—Has little or no affect on unit effectiveness

OGA

| | Answer No. 1 | | Answer No. 2 | | Answer No. 3 | |
|---|---|---|---|---|---|---|
| | Number of Responses | Percent of Total | Number of Responses | Percent of Total | Number of Responses | Percent of Total |
| Overall | 463 | 58.5 | 173 | 22.0 | 152 | 19.2 |
| Army | 220 | 78.9 | 23 | 8.2 | 36 | 12.9 |
| Navy | 99 | 68.2 | 25 | 17.5 | 19 | 13.3 |
| Air Force | 199 | 37.1 | 118 | 36.8 | 84 | 26.2 |
| Marines | 25 | 55.6 | 7 | 15.6 | 13 | 28.9 |

~~(C)~~ Listed below are a number of factors which might tend to cause responsible persons to avoid taking TSV equipments into combat or simulated combat. Rank them (and any others you may wish to add) in the order of their importance to you.

A—My military career might suffer if I were judged responsible for the loss or compromise of cryptographic material.

B—The enemy might be able to recover lost equipment and keying materials and might then be able to read U.S. TSV traffic.

C—If my TSV equipment were lost at a critical time, its unavailability might reduce the operational capability of my unit.

D—The TSV my unit uses most must be *carried* into combat and is so heavy that it slows down our mobility.

E—Other (Specify)

| | A | B | C | D | E | |
|---|---|---|---|---|---|---|
| Overall | 45 | 266 | 87 | 63 | 29 | |
| Army | 24 | 113 | 43 | 47 | 5 | Figures shown |
| Navy | 7 | 31 | 19 | 0 | 3 | are first |
| Air Force | 13 | 104 | 21 | 3 | 10 | choices |
| Marines | 1 | 18 | 4 | 13 | 1 | |

~~(C)~~ If you use TSV equipment in combat, simulated combat, or other hazardous circumstances, does your concern about its possible loss or compromise restrict its operational use or usefulness?

1—Yes, to a considerable degree

2—To some moderate degree but not significantly

3—No

| | Answer No. 1 | | Answer No. 2 | | Answer No. 3 | |
|---|---|---|---|---|---|---|
| | Number of Responses | Percent of Total | Number of Responses | Percent of Total | Number of Responses | Percent of Total |
| Overall | 46 | 7.7 | 97 | 16.3 | 451 | 75.9 |
| Army | 30 | 13.6 | 57 | 25.9 | 133 | 60.5 |
| Navy | 2 | 2.6 | 10 | 13.0 | 65 | 84.4 |
| Air Force | 7 | 2.9 | 2 | 0.8 | 229 | 96.2 |
| Marines | 7 | 17.9 | 8 | 20.5 | 24 | 61.5 |

~~(C) Listed~~ below are a number of possible operational disadvantages which have been raised with regard to the use of TSV communication and identify their importance to you.

A—Inability of TSV-equipped stations to communicate in cipher with all desired stations.

B—Occasional interruption of communication due to loss of synchronism between the transmitting and receiving stations.

C—The time delay required to synchronize the sending and receiving crypto-equipments is intolerable in some type of military activity.

D—The size and weight of the TSV equipments and their power supplies is prohibitive in some situations.

E—The application of TSV equipment to UHF, VHF-AM, and/or VHF-FM tactical radio circuits/nets reduces seriously the effective ranges.

F—An unacceptable level of maintenance problems are associated with the operation of TSV equipments.

G—TSV equipment is not reliable in critical situations.

H—Unacceptable physical security restrictions are associated with the use of TSV equipments in the field.

I—Other (Specify)

| | A | B | C | D | E | F | G | H | I |
|---|---|---|---|---|---|---|---|---|---|
| Overall | 223 | 115 | 46 | 54 | 31 | 18 | 28 | 13 | 12 |
| Army | 72 | 43 | 7 | 39 | 10 | 11 | 1 | 5 | 2 |
| Navy | 41 | 31 | 6 | 1 | 7 | 3 | 7 | 3 | 4 |
| Air Force | 101 | 35 | 30 | 4 | 14 | 4 | 20 | 4 | 4 |
| Marines | 9 | 6 | 3 | 10 | 0 | 0 | 0 | 1 | 2 |

~~(C)~~ From the NESTOR experience, and the antithetical experience with ORESTES and other systems in much the same environments, it might be concluded that the overriding criteria for the acceptance or failure of our equipment offerings are whether there is a perceived need and whether they do what they're supposed to do – they work – reasonably well without inhibiting operations.

## EMERGENCY DESTRUCTION OF CRYPTO-EQUIPMENT

~~(C)~~ Except in a tiny number of locations where the user can afford the luxury of large powerful disintegrators that chew crypto-components into little pieces, we remain dependent on World War II pyrotechnic technology to get rid of crypto-equipments in a hurry in an emergency. Meanwhile, the environments into which the equipments are now being deployed are increasingly hazardous in peace time and in war. Further, when we ruggedize hardware we aren't kidding, having fielded some of the most indestructible boxes in the world. Some seem at least on a par with flight recorders that survive the most catastrophic of crashes.

~~(C)~~ A crashed helicopter in Vietnam caught fire and reduced itself to not much more than slag. Its NESTOR equipment was fished out, cleaned up, and ran perfectly. More recently, a telemetry encryption equipment (KG-66) on a missile shot at White Sands ran perfectly after being dug out of the 8 foot hole created at impact.

~~(C)~~ Chip technology compounds the problem. The chips are so small that they'll often filter through a disintegrator unscathed. Conventional pyrotechnics don't help because their melting temperature is typically 2800° F.

~~(S-NF)~~ Meanwhile, the new environment? When Volume I was written, the only case in US history of the invasion of an Embassy was by mob in Taipeh in 1957. There were no destruct facilities and, had there been, then as now, the whole building would have gone up in smoke had pyrotechnics been used. So – again then as now – reliance was on the vault. Since the mob could not penetrate its big steel door, they knocked a hole in the adjacent wall, stormed into the crypto-center, and scaled rotor and other cryptomaterial down to the crowd below. About 50 of the 100 or so rotors were not seen again. Since those days, no less than 32 (counting MAAG, the total is near 50) U.S. facilities (embassies, legations, missions) containing crypto-equipment have come under attack, 13 of them during the 6 Day War in the Middle East, 7 more in Iran during the revolution, another incident with the re-invasion of the Embassy when the hostages were taken, other assaults in Islamabad and Tripoli, and an attempt on our Embassy in Beirut.

~~(S-NF)~~ In all, in the first Iranian crisis, 7 different types of crypto-equipment were jeopardized, totalling some 65 pieces of hardware. Precautionary evacuation and emergency destruction efforts ranged from total and sometimes spectacular success, to complete failure in one installation where two types of equipment had to be left up, keyed, running, and intact. It became clear that our destruct capabilities were inadequate or useless where we had little warning, and hazardous at best even where warning or a good vault offered time to carry out the procedures. Fire could lead to self-immolation in the vaults; shredders and disintegrators depended sometimes on outside power which was cut off; and smashing of equipments could render them inoperative, but not prevent the reconstruction of their circuitry.

~~(S)~~ Correlatively, our traditional policy for limiting the use of crypto-equipments in "high-risk" environments was quite evidently wanting. That policy generally called for deployment of our oldest, least sensitive, and usually, least efficient systems in such environments. The effect was to deny people in the field good equipment in crisis, just when they needed it most. This was particularly true of secure voice equipment to report events, and effect command and control when installations were under attack.

~~(C)~~ What seems needed is some push-button capability to zap the equipment, literally at the last moment, allowing secure communications until the facility must be abandoned, and not dangerous to the button pusher.

~~(S)~~ The most successful use of pyrotechnics (thermate slabs, thermite grenades, and sodium nitrate barrels) in Teheran occurred at the major Army Communications Center there. It had a number of crypto-equipments, but also served as a depot for pyrotechnic materials for the whole area. They piled all of their classified cryptomaterial in a shed; covered them with their pyrotechnic material (some 300 devices), lit off the whole enchilada, and took off. The result was probably the largest single conflagration during the entire revolution. Observers reported seeing flames shooting hundreds of feet into the air from posts several miles away. The building was, of course, consumed, and we assume only a slag pile remains. (At this writing, about 15 months later, no American has been back.)

~~(S)~~ Despite all of the above, we have not been altogether inert on the matter of emergency destruction over the past decade or so. Each catastrophe seems to have stimulated at least a brief burst of effort to find a way. When the Pueblo was captured, we found that our best laid emergency destruction plans had gone awry. There was a shredder and an incinerator on board, and a few axes and sledges. In those days, Navy ships were not permitted to carry pyrotechnic destructors because of their fire hazard. Considerable reliance was placed on jettisoning material; but in the Pueblo case, the crew could not get to the side without being machine-gunned. We had, in any event, become increasingly skeptical of jettisoning as a viable way to prevent the recovery of equipment as various submersibles attained greater and greater depths. We also found to our astonishment that some of the electronic crypto-equipments built in the fifties (and sixties) *float.*

~~(S)~~ Our first major customer for a safe and reliable means for emergency destruction on shipboard was, as you might expect, another intelligence collector [redacted] S2 was allowed to fabricate some boxes (on a not-to-interfere with COMSEC work basis) which would incinerate material while containing the heat and flame. Some research was carried out, again under S2 aegis, to build or modify ordinary safes to destroy their own contents. Work came to a virtual halt, however, when a disgruntled contractor whose proposal had been turned down raised an unholy stink with our Director, senior officials in the Defense Department, and sundry Congressmen. (Congressional inquiries, we have discovered, can sometimes have a chilling effect.)

~~(C)~~ The upshot was that NSA and DoD decided that the *general* problem of destroying classified materials was not NSA's business – particularly with respect to the destruction of ordinary classified documents. We were directed to confine ourselves exclusively to techniques uniquely useful in the cryptographic business. The trouble was that there was no other Government Agency prepared to accept such a role. The Army Chemical Corps had provided the original pyrotechnic approaches to destruction but, as noted, had not done much since World War II except, at NSA behest, the development of the sodium nitrate in a barrel or hole-in-the-ground approach. There had been an agency created in the Department of Defense in its early days called the Physical Security Equipment Agency. It was an assemblage of physicists, chemists, and engineers with little security background and apparently, few practical ideas. They were abolished in December 1976, with no re-assignment of their functions.

~~(C)~~ So, in 1976, DoD accepted the overall responsibility for destruction methodology, and assigned the Navy as Executive Agent to do the necessary research and development. As usual, they were underfunded and understaffed, and have been progressing very slowly. We, meanwhile, keep not much more than a manyear or two engaged in the special problems of crypto-equipment destruction. With our increasing reliance on micro-circuitry, someone had the idea of planting tiny, non-violent shaped charges in critical junctures in our circuits that could be triggered by the application of external voltage. The project became known as LOPPER, and R1 was charged to pursue it. The original equipment targetted for incorporation of the technique was VINSON. But, it would cost more, might delay the program and, again, did we really need it? So, R1 had developed the technique to the point of feasibility demonstration models; tests were run on circuit boards, were successful, and we stopped.

~~(C)~~ We were damned again by the perception that this was a solution looking for a problem – exactly the same inhibiter which has slowed or killed nearly every new departure that costs something for which there is no *universally* recognized need. We (proponents of the desirability of protecting our hardware as best we can for as long as we can) had done it to ourselves when we began letting people know, as early as 1950, that the key's the thing; all those contrary arguments in the direction on classification nonwithstanding. One set of curmudgeons in our business can insist that security is not free, that we are in the communications security not the communications economy business, while another set, with equal force, can state that the too-high security standards or demands are pricing us out of the market, leaving our tender communications altogether naked to the world.

(U) I suggest that newcomers to the business not jump on board whichever side of this controversy your viscera may first direct. Rather, take the other side – whichever it is – and go through the exercise of building its defense. You are likely to be surprised at how elaborate and involuted the arguments become either way and might lead you to my personal conclusion that the best way to achieve a net gain in our resistance to communications compromise is through compromise. Still, it seems that once in a while one



EO 1.4.(c)

ought stand on principle – as a matter of principle! – and hang tough where truly vital interests are concerned.

~~(C)~~ So, LOPPER came a-cropper, at least for a time. The "compromise" solution was put forward: if we can't afford to implant this technology in the whole product line, can't we at least build a limited quantity of circuit boards with the capability for deployment to high-risk facilities? The answer was no: small quantity production is far too expensive; you can't amortize the R&D and product costs. Turns out that there is a useful rule of thumb for most of our product line: unit cost drops 15–20% for each doubling of the number of procured.

(U) At the moment, we are in low-key pursuit of a variation of the LOPPER approach for some future systems. It involves burying a resistor in the chip substrates which will incinerate micro-circuitry with the application of external voltage. We'll see.

THIS PAGE IS INTENTIONALLY BLANK

## POSTSCRIPT ON DESTRUCTION—DAMAGE ASSESSMENTS

~~(C)~~ When major potential losses of cryptomaterial occur, damage assessments are called for – usually in a hurry; and particularly if the possibly compromising incident hits the press. Often, we will have 24 hours or less to make some kind of interim assessment of what may have been lost, in what quantity, with what probability, and with what impact on national security.

~~(C) O~~ften in this hectic process, we start out with little more than what's in the newspapers but, because of our access to the records of the crypto-accounts involved, we are usually able to build a pretty good inventory of the materials involved within a few hours and, sometimes have information on the destruction capabilities at the site(s) involved. In first reports, what we rarely get is an accurate picture of the degree of the destruction actually achieved; so our initial assessments are invariable iffy.

~~(C)~~ A principal lesson we have learned in formulating these assessments is patience – sometimes waiting many months before we "close" the case, meanwhile interviewing witnesses to or participants in the event, visiting the scene if we can get there, performing laboratory analyses of recovered residues of the destruction effort, and so on, before making a definitive declaration of compromise or no compromise, as the case may be.

~~(C)~~ A second lesson has been that our first gut reactions have usually been wrong, erring equally on the optimistic and pessimistic sides when all the facts (or all the facts we're ever going to get) are in. Some materials have been recovered after many days, weeks, or months under hostile control with no evidence that they knew or cared what they had. In other cases, post mortems have shown losses to have been significantly more substantial than were suggested by the early "facts."

~~(C) F~~inally, we have found it prudent to treat damage assessments as exceptionally sensitive documents, for two reasons. The first is that they explain just what the materials are and how they could be exploited by a canny opponent. The second is that they reveal our own judgment on what was and wasn't lost. That information is important to any enemy, particularly if we were wrong, and he has been able to recover something we think he does not have.

THIS PAGE IS INTENTIONALLY BLANK

## TRANSPOSITION SYSTEMS REVISITED

(C) In Volume I, it was noted that transposition systems were thrown out of our lexicon because they contained the seeds of their own destruction – all of the elements of plain language appear in the cipher text; they've merely been moved around with respect to one another. A jigsaw puzzle, in fact.

(C) Turns out, the same deficiency exists with equipments designed to destroy classified paper by shredding and chopping it into small pieces. The spectacle, in early 1980, of Iranian "students" occupying the US Embassy in Teheran, laboriously fitting together shredded materials comes to mind. In the destruction world, the problem was more or less solved by insisting that the pieces be so small and numerous that worlds of work would produce only fragmentary results.

(S) Our current standard – no destruction machine approved unless the resultant fragments were no larger than 1.2 mm x 13 mm (or 0.73 mm x 22.2 mm depending on the crosscut shredder used) was arrived at viscerally. But when the technology came along, we verified the standard by investigating the computer-assisted edge-matching or similar techniques which could see and remember shapes in a large display of small two-dimensional objects, and sort out those that fit together. As a result, we feel more comfortable about the question of whether such stuff can be reconstructed, however painstaking the attack. (As always, though, there are pressures to relax the standard, allow larger chunks because the finer the grain you demand, the more costly and time consuming the process. In a chopper, for example, you need more and finer blades, finer screens, and more cycling of the machine.) The material in Teheran by the way, was not from the crypto-center and was the product of a machine which we had specifically disapproved for our purposes.

(C) The transposition idea for cryptography did not stay dead with us. It had enormous attraction in the voice encryption business because if elements of speech could simply be arranged (transposed) in time and/or frequency, that would eliminate the need for digitization, which would in turn save bandwidth and still give good fidelity when it was unscrambled (untransposed). That meant enciphered voice of reasonable quality could be driven through narrowband transmission systems like ordinary telephone circuits and HF radio. Long-haul voice communications would be possible without large, complex very expensive terminals to digitize and still get the fidelity required.

(S) So, PARKHILL. Instead of making our fragments physically small as in a paper destructor, we made them small in time – presenting a brand new jigsaw puzzle each 1/10th of a second. Solvable? Sure. All you have to do is reconstruct 600 completely separate and quite difficult cryptograms for each minute of speech. We calculate that a good analyst might do a few seconds worth a day. Looks to be a risk worth taking – with that plain language alternative staring us in the face. We did, however, impose some limits in its use.

(S) We had never before fielded a less than fully secure crypto-equipment and, as our various caveats on its security limitations were promulgated, they sent some shock waves through the customer world and caused some internal stress in S. Our applications people quite rightly sought maximum use where plain language was the only alternative, while security analysts (also rightly) expressed continuing reservations on whether its usage could really be confined to tactical and perishable traffic – particularly as it gravitated increasingly towards wireline application rather than just HF radio for which it was originally designed.

(S) Part of the difficulty may have been that the only formal, objective crypto-security *standard* ever published in S is the High Grade Standard for equipments – systems meeting that standard are essentially approved for any type of traffic you might specify for their fifteen or twenty year life. No intermediate or "low-grade" standard has been adopted, despite yeoman efforts to devise one. Ironically, even among the high grade systems, there is considerable variation in their overall security potential – some provide kind of traffic they can process. At this writing, however, rumor has it that there is a sub-rosa paper authored by a fresh face entitled something like: "Manual systems – Are they Worth the Paper They're Printed On?" COMSEC will be well-served with critical re-examination of old ideas and quite a batch of hoary premises (including some in Volume I!), particularly by our new people. Just be sure of your facts.

## MORE MURPHY'S LAW

~~(S)~~ There have been occasions when we have had reason to suspect unauthorized access to various cryptomaterials which we could not prove. In these circumstances, if we can recover the material in question, we are likely to subject it to laboratory analysis to see if we can find evidence of tampering, unexplained fingerprints, and so on. One such case involved an operational T.S. key list being examined for latent prints in an S2 chemical lab. When the document was placed on a bench under the powerful blower system used to evacuate fumes at that position, this highly sensitive strictly accountable item was sucked up and disappeared into the elaborate duct-work system above the false ceiling.

~~(C)~~ For NSA to have lost that keylist would have been a matter of acute embarrassment and there was, thus, considerable milling about. People were dispatched to the roof to check the vent with visions of our key list wafting somewhere about the wilds of Fort Meade. The vent was screened, however, and the document had not come up that far – it was somewhere in the bowels of the building in several hundred feet of ducting. GSA technicians arrived, and work was started from the bottom. At the first elbow, there was a small jam of paper, cotton, and cleaning rags, but no key list. About 20 feet along at another sharp bend, tin snips were used to open up the duct, and there was the document, snagged on some jagged protuberance. A relieved custodian clutched the document, and no compromise was declared.

~~(C)~~ An automobile crashed in Texas and the trunk sprang open. State troopers found a suspicious-looking duffle bag and checked its contents. Hundreds of low-level Op-Codes and authenticators were inside. The driver claimed not to have known the material was there; the car belonged to his brother-in-law, a Sergeant who had been shipped to Vietnam a few months earlier. He was tracked down and, sure enough, had left the material in the trunk for the duration. He had evidently been on a run to the incinerator with a burnbag full of used materials, had run out of time, and shipped out leaving the chore undone. He claimed he intended to get rid of the stuff when he got back.

~~(S)~~ Somebody moved into a small apartment near a Navy base in California. Far back on a top closet shelf he found a clip-board. On the board were two T.S. ADONIS keylists and several classified messages. The previous resident, a military man, had occupied the apartment only briefly, and swore he had never seen the material in his life. The origin of the keying material was traceable by short title, edition, and *register number*, and turned out to have been issued to a unit at Camp Lejeune.

~~(S)~~ More research showed that a Marine Sgt who had had access to the material had been sent to the West Coast, and sure enough, had lived for a while in the apartment where the documents were found. He was located and admitted that he had squirreled the material away, and claimed he had then forgotten it. His motive? Simply that classified documents "fascinated" him.

~~(C)~~ Strangely enough, this is a recurring theme. In this case, the polygraph seemed to bear him out, as it did in at least one other case where the identical motivation was claimed.



P.L. 86-36

jettison as a way to get rid of our stuff unless at very great depths and in completely secret locations. (Shortly after WWII, small Army training crypto-devices called the SIGFOY were disposed of beyond the 100 fathom curve off Norfolk. Some years later, they became prize souvenirs for beach combers as they began washing ashore.)

~~(C)~~ *UNSOLVED PUZZLE* – We used to store a lot of cryptomaterial in a warehouse at Ft. Holabird. It was fenced and protected by a 24-hour armed civilian guard. One evening, such a guard saw an individual inside the fence, evidently attempting to penetrate the warehouse. He drew his weapon, cried "Halt!" and led the individual to the guard shack and started to call in for help. About that time, the intruder started running, climbed the fence, and disappeared. We asked the guard why he didn't shoot – he said he was afraid he might hurt somebody. It was one of the few attempted penetrations we know of, and has never been resolved.

~~(C)~~ *CONFETTI* – When we manufacture one-time tape, a by-product of the punching process is millions upon millions of tiny, perfectly circular pieces of paper called "chad" that come out of holes in the tape. This chad was collected in burn bags and disposed of. Someone thought it would make good public relations to give this stuff to high school kids for use as confetti at football games. Inevitably, one of the burn bags was not quite empty when the chad went in. At the bottom, were a couple of TOP SECRET key card book covers and a few assorted keys. They carried the impressive caveats of those days like "CRYPTO – CRYPTO-CLEARANCE REQUIRED" and were, to use a term earlier referred to, "fascinating" to the kids when they discovered them.

~~(C)~~ One of the girls, whose father happened to be an Army officer, tacked some of this material on her souvenir board. When Daddy saw it, he spiralled upward. He decided that it must be destroyed immediately; but first made a photograph of it for the record. He tore it up, flushed it away, and reported in. With some difficulty, various cheerleaders and other students who had glommed on to some of this material were tracked down, and persuaded to part with it. We no longer issue confetti.

~~(C)~~ We used to keep careful records of security violations in S, publicize them, and run little contests to see what organization could go longest without one. A retired Lt. Colonel wrecked S1's outstanding record as follows:

~~(C)~~ He reported to work one morning and found one of those ominous little slips on his desk, asserting that a paper under his blotter carried a safe combination, and "requesting" him to report to Security at once. He was outraged – he had never been guilty of a security violation in his life; the safe combination was not his, nor did it match any safe in his office. He rushed out the door and down to the Security Office. They accepted his story, cancelled the "violation," and he returned to his office somewhat mollified.

(U) There, on his desk, was another violation slip. He had left his office door open when he reported to security, and that was against the rules. That one stuck.

~~(C)~~ A (now) very senior official in S bent the rules by starting out to a conference in the Pentagon with some classified papers but without escort. He got as far as Foxhall Road in an ice-storm where he was confronted with a pile-up of cars that had skidded uncontrollably down into the hollow adjacent to the Girls' School there. He managed to slide to a stop without adding to the pile, got out, and immediately found himself in the path of a following car skidding toward him. To see him now, you would not believe that he made the only route to safety – over the seven foot chain link barbwire-topped fence around the school. He got some lacerations in the process, however, and someone took him to Georgetown Hospital for treatment. He refused to go, however, until he was able to flag down an NSA employee (our Adjutant General at the time!) to take custody of his classified materials.

~~(C)~~ There have been, by the way, rather serious incidents involving classified materials in automobiles. In one case, an individual carefully locked a briefcase full of classified reports in the trunk of his car while he made a quick stop at a business establishment. The car was stolen while he was inside. So, watch it.

~~(C)~~ When technical security teams "sweep" our premises, one of their chores is to examine conduits for extraneous wires, trace them out, or remove them. We had a peculiar case at Nebraska Avenue (the Naval Security Station at Ward Circle where various parts of the Agency were tenants from 1950 until 1968). An inspector on the third floor removed a floor access plate to examine the telephone wiring and saw a wire begin to move. He grabbed it, retrieved a few feet, then unknown forces on the other end began hauling it back. A tug of war ensued. Turned out that a fellow-inspector on the floor below was on the other end.

**CLASSIFIED TRASH**

~~(C)~~ One day, back in the '60's, one of our people was poking about in the residue baside the Arlington Hall incinerator. The incinerator had been a headache for years: the screen at the top of the stack had a habit of burning through and then it would spew partially burned classified COMSEC and SIGINT materials round and about the Post and surrounding neighborhood. Troops would then engage in a giant game of fity-two pickup. This day, however, the problem was different – the grate at the floor of the incinerator had burnt out and the partially burned material, some the size of the palm of your hand, was intermixed with the ash and slag.

~~(C)~~ There was no way of telling how long the condition had persisted before discovery, so we thought we had better trace the ash to the disposal site to see what else was to be found. The procedure was to wet down the residue for compaction, load it on a dump truck, and haul it away. In the old days it had evidently beem dumped by contractors in abandoned clay pits somewhere in Fairfax County (and we never found them); but the then current practice was to dump it in a large open area on Ft Meyer, South Post, adjacent to Washington Boulevard.

~~(C)~~ Our investigator found that site, alright, and there discovered two mounds of soggy ash and assorted debris each averaging five feet in height, eight to ten feet wide, and extending over 100 yards in length. He poked at random with a sharp stick, and thought disconsolately of our shredding standards. Legible material was everywhere – fragments of superseded codes and keying material, intriguing bits of computer tabluations; whole code words and tiny pieces of text. Most were thumb-size or smaller; but a few were much larger. Other pokers joined him and confirmed that the entire deposit was riddled with the stuff. Some of it had been picked out by the wind and was lodged along the length of the anchor fence separating the Post from the boulevard.

(U) Our begrimed action officer was directed to get rid of it. *All* of it. Being a genius, he did, and at nominal cost. How did he do it?

~~(S)~~ The solution to this problem was most ingenious – a truly admirable example of how a special talent combined with a most fortuitous circumstance eventually allowed us to get all that stuff disposed of. I won't tell you the answer outright: instead, I will try to aggravate you with a very simple problem in analysis of an innocent text system. Innocent text systems are used to send concealed messages in some ordinary literature or correspondence. By about this time, you may suspect that perhaps I have written a secret message here by way of example. That, right, I have! What's here, in fact, is a hidden message which gives you the explanation of the solution we accepted for disposing of that batch of residue. If we ever have to do it that way again, it will be much more difficult for us because the cost of everything has escalated, and I doubt we could afford the particular approach we took that time.

~~(S)~~ If you are really interested in how innocent text systems are constructed, he advised that there are twenty-jillion ways to do it – every one of them different. Some of them may use squares or matrices containing an encoded text with their values represented by the coordinates of each letter. Then those coordinates are buried in the text. About another million ways – a myriad – are available for that last step. In fact, the security of these systems stems mostly from the large variety of methods that can be used and on keeping the method (the logic) secret in each case. Once you know the rules, solution is easy. So now, find my answer above – no clues, except that it's very simple, and one error has been deliberately incorporated, because that is par for the course.

THIS PAGE IS INTENTIONALLY BLANK