Description of document:	**21 Articles from (various issues of the) National Security Agency Technical Journal**
Requested date:	30-September-2006
Released date:	11-January-2008
Posted date:	06-February-2008
Date/date range of document:	1957 – 1965
Source of document:	NSA FOIA Requester Service Center: National Security Agency Attn: FOIA/PA Office (DJ4) 9800 Savage Road, Suite 6248 Ft. George G. Meade, MD 20755-6248 Telephone: (301) 688-6527 Fax: (443) 479-3612
Notes:	See list of articles included in release letter, following page Updated 09-March-2008 Article: Soviet Science and Technology: Present Levels and Future Prospects released and added to this file

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

FOIA Case: 51551A
11 January 2008

This further responds to your Freedom of Information Act (FOIA) request of 30 September 2006 for the following NSA Technical Journal articles:

- "Development of Automatic Telegraph Switching Systems" (Vol. II, No. 3, July 1957)
- "Chatter Patterns: A Last Resort" (Vol. II, No. 4, October 1957)
- "Introduction to Traffic Analysis" (Vol. III, No. 2, April 1958)
- "Science and Cryptology" (Vol. III, No. 3, July 1958)
- "A New Concept in Computing" (Vol. III, No. 4, December 1958)
- "About NSA" (Vol. IV, No. 1, January 1959)
- "Data Transmission over Telephone Circuits" (Vol. IV, No. 1, January 1959)
- "Antipodal Propagation" (Vol. IV, No. 1, January 1959)
- "Soviet Science and Technology: Present Levels and Future Prospects" (Vol. IV, No. 1, January 1959)
- "The Borders of Cryptology" (Vol. IV, No. 4, October 1959)
- "A Program for Correcting Spelling Errors" (Vol. IV, No. 4, October 1959)
- "Don't Be Too Smart" (January 1960)
- "Did Alexander Popov Invent Radio? " (January 1960)
- "Book Review: "Lost Languages" (Fall 1960)
- "Aristocrat - An Intelligence Test for Computers" (Vol. VII, No. 2, Spring 1962)
- "A Cryptologic Fairy Tale" (Vol. VII, No. 2, Spring 1962)
- "Why Analog Computation?" (Vol. VII, No. 3, Summer 1962)
- "Book Reviews: Various" (Vol. VIII, No. 1, Winter 1963)
- "Soviet Communications Journals as Sources of Intelligence" (Vol. IX, No. 3, August 1964)
- "Something May Rub Off!!" (Vol. X, No. 1, Winter 1965)
- "Time Is - Time Was - Time Is Past: Computers for Intelligence" (Vol. X, No. 1, Winter 1965)

For purposes of this request and based on the information you provided in your letter, you are considered an "all other" requester. As such, you are allowed 2 hours of search and the duplication of 100 pages at no cost. Since processing fees were minimal, no fees were assessed. Your request has been processed under the FOIA, and all but two of the documents you requested are enclosed. Certain information has been deleted from the enclosures, and one document ("Don't Be Too Smart," 3 pages in all) has been withheld in its entirety. "A Cryptologic Fairy Tale" was previously reviewed and released under the Mandatory Declassification Review (MDR) requirements of Executive Order (E.O.) 12958, as amended. That article is provided to you as it was released in MDR Case 52172.

Some of the information deleted from the enclosed documents was found to be currently and properly classified in accordance with Executive Order 12958, as amended. This information meets the criteria for classification as set forth in Subparagraphs (c) and (g) of Section 1.4 and remains classified TOP SECRET, SECRET, and CONFIDENTIAL as provided in Section 1.2 of the Executive Order. The information is classified because its disclosure could reasonably be expected to cause exceptionally grave damage to the national security. The information is exempt from automatic declassification in accordance with Section 3.3(b)(1), (b)(3), and (b)(8) of E.O. 12958, as amended. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. Section 552(b)(1)).

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in these documents. Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 403-1(i); and Section 6, Public Law 86-36 (50 U.S. Code 402 note).

Since one document was withheld in its entirety and information was withheld from the enclosures, you may construe this as a partial denial of your request. You are hereby advised of this Agency's appeal procedures. Any person denied access to information may file an appeal to the NSA/CSS Freedom of Information Act Appeal Authority. The appeal must be postmarked no later than 60 calendar days from the date of the initial denial letter. The appeal shall be in writing addressed to the NSA/CSS FOIA Appeal Authority (DJP4), National Security Agency, 9800 Savage Road STE 6248, Fort George G. Meade, MD 20755-6248. The appeal shall reference the initial denial of access and shall contain, in sufficient detail and particularity, the grounds upon which the requester believes release of the information is required. The NSA/CSS Appeal Authority will endeavor to respond to the appeal within 20 working days after receipt, absent any unusual circumstances.

FOIA Case: 51551A

Please be advised that the article "Soviet Science and Technology: Present Levels and Future Prospects" contains other government agencies' information. Because we are unable to make determinations as to the releasability of the other agencies' information, the subject document has been referred to the appropriate agencies for review. We will respond to you further when consultation with the other agencies has been completed.

Sincerely,

Pamela C. Phillips
for

RHEA D. SIERS
Deputy Associate Director for Policy

Encls:
a/s

Development of Automatic Telegraph Switching Systems

BY R. D. PARKER

Unclassified

There are two general types of automatic telegraph switching systems. In one, electrical circuits are established to provide communication paths between telegraph stations in customers' offices and are broken when the need for communication is over. In the other, direct electrical circuits between stations are not established, but coded information in messages automatically routes them through telegraph networks to their destinations. This paper describes briefly some of the systems now in use, and outlines some of the requirements which had to be met to provide a satisfactory service.

INTRODUCTION

A switch as used in electrical engineering is defined in dictionaries as a device for making, breaking, or changing the connections in an electric circuit. When a switching operation is performed, circuits are changed from one connection to another and devices are cut in and out of circuits. The idea is to transfer or shift these electrical circuits and devices around.

A telephone central office or exchange is an excellent example of the above, in that electrical voice-transmission circuits are shifted about to establish communication paths between parties, and are broken when conversations are over. Thus, a telephone exchange area such as the District of Columbia is operated as a large electrical switching system.

Telegraph circuits are established, broken, and shifted around like telephone circuits, and when telegraph circuits to subscribers' premises are connected and disconnected on requests from subscribers a telegraph exchange system is created. In telegraphy, however, another concept of switching has grown up. This is because telegraph messages, as contrasted with telephone messages, can easily be stored, held in transit, and re-transmitted sometime after reception. The pieces of paper or other message recordings are the things shifted or switched around. A telegraph office where messages on blanks are shifted from an incoming circuit to one or more of several outgoing circuits has been called a "relay" office, in that received messages are later transmitted to their destinations, but, such an office is also in fact a message-switching center. A "relay" office does indeed suggest a relay race, in which a baton is handed at a point of exchange to the next runner; but this comparison fails to take into account the switching which is performed in telegraphy. If in a relay race each baton carried a coded message which had to be decoded at the exchange point to determine which runner of a group would carry a particular baton for the next lap and batons were passed accordingly the analogy would be more complete. This imagined reshuffling of batons is message switching.

In recent years a new technical development has permitted telegraph messages to be routed or directed *automatically* from their point of origin to their destination by means of coded electrical impulses which are in a sense part of the message but precede the normal address, the text, and the signature. An arrangement following this method of working, with a center where messages are stored, analyzed, and retransmitted, becomes, therefore, an automatic message-switching system. The circuit arrangements are fixed and the messages are switched. This operation may be electromechanical or electromagnetic, with messages stored by perforated tape, on magnetic tapes and drums or some other manner, but direct electrical paths between sending stations and addressees are never established.

Thus telegraphy, unlike telephony, has two types of switching systems, one, circuit switching and the other, message switching, each with its own problems. Accordingly, it is desirable to consider them under separate sections: Section I, Circuit Switching; and Section II, Automatic Message Switching.

SECTION I—CIRCUIT SWITCHING

GENERAL

There are two well established systems operating today in which printing-telegraph circuits are switched to provide direct communication paths between subscriber stations: one in America, known as Teletypewriter Exchange Service or TWX, and the other in Europe, started as a national service but now rapidly expanding on an international basis, and known as TELEX[1]. TWX was initiated in the early 1930's and TELEX followed with the first installations in England.

Shortly after World War I, when the writer started the development of printing-telegraph switching systems for the American Telephone and Telegraph Company, he was informed by General J. J. Carty, who was then head of its Development and Research Department, that before the introduction of the telephone in the latter part of the 1870's a rather extensive telegraph switching system was in operation in New York City. In this system, Morse circuits from a central exchange radiated to customer's offices. Each customer hired a Morse operator, who handled messages and requested the central-exchange operator to make circuit connections to other customers. The advent of the telephone, saving the expense of the Morse operators, quickly put an end to this type of telegraph switching.

The actual introduction of a printing-telegraph switching or exchange public service had to wait for the development of a satisfactory start-stop type of telegraph printer, teletypewriter, teleprinter or, teletype machine, as it is variously called. It is reasonable to ask what is meant by "start-stop" and why it is important in planning an exchange system. Start-stop means a method of operating printing-telegraph machines in which the code group needed for selecting a character is preceded by an impulse, always of the same kind, which indicates to a receiver that a code group representing a character will follow immediately. This simple impulse is the "start". Furthermore the code group is followed by an impulse opposite in kind to the start, which brings the receiver to a rest condition in preparation for the next start impulse. This final impulse in the complete sequence for each character is the "stop". Sending and receiving machines do not operate at exactly the same speed, and without the start-stop feature a receiver would quickly gain or lose enough relative to a sender to cause errors in the received copy. A fresh start at each character keeps the machines in good relationship with each other and prevents these errors. Most printing-telegraph machines in use today operate on this principle. Such machines operating at about the same speed in words per minute and having like code character combinations may be freely interconnected by electrical circuits for a typed form of communication service. Thus, with the "start-stop" code a printing-telegraph circuit-switching system became feasible.

BELL SYSTEM TWX SERVICE

The Bell System established a public nation-wide printing telegraph switching service in 1931, following a long development and trial program. It was realized that little or no local business could be expected, and because of the necessity for recording and later billing customers for long distance calls, manually operated toll switchboards were especially designed for the service. All communications between toll-operators in distant cities, and between operators and subscribers, were made by means of printing-telegraph machines. The typed records proved to be of assistance to operators in spite of the slow speed

[1] TEX is the abbreviation adopted by the Radio Corporation of America for its overseas Teleprinter Exchange Service and associated TELEX stations in Europe and other areas.

of the machines—60 words per minute—as compared with speech, and the time required to establish toll-connections was found to be essentially the same as that for manual toll-telephone service.

A simple intercity TWX connection is illustrated in Fig. 1. Station A in New York is electrically connected to Station B in San Francisco so that coded signals for typing and machine control purposes may be passed back and forth to give a typed-record form of communication service. A call is initiated by a subscriber's turning on the power switch of the teletypewriter station set. This signals the switchboard operator, who requests the number of the called party by operating the keyboard of a machine which is an integral part of the switchboard. The party originating the call types this information, the operator selects a trunk to the distant city and passes the called number by typing to the incoming operator, who connects the trunk to the called station line and rings the station bell. Toll tickets are made out for billing purposes as with telephone service. Disconnect signals are flashed to the operators by the act of turning off the power-switch at either subscriber's station.

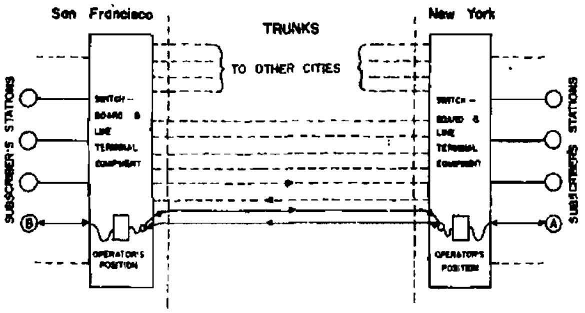


Fig. 1—Teletypewriter Exchange Service—Simple Intercity Call

When a connection such as is illustrated in Fig. 1 is established, subscribers may "talk" back and forth on a conversational basis, except that they use keyboards and their "conversation" is in typed form. A receiver may interrupt a sender and obtain control of the circuit by transmitting a "break signal" against the incoming signals and "locking out" the sending keyboard. Station equipment with perforated tape may also be employed where considerable message traffic is handled.

Over the years, automatic features have been added to the original manual scheme, and in many cases certain switching operations are performed under the control of impulses transmitted over the communication circuits. An example is the use of a "concentrator", placed in a local area where a number of TWX subscribers are grouped. The concentrator is arranged to associate these subscribers automatically with trunks to a main TWX switchboard at some distant point.

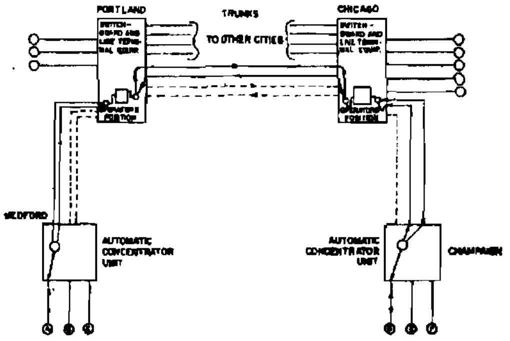

PORTLAND
TRUNKS
CHICAGO
SWITCH-BOARD AND LINE TERMINAL EQUIP.
TO OTHER CITIES
SWITCH-BOARD AND LINE TERMINAL EQUIP.
OPERATOR'S POSITION
OPERATOR'S POSITION
MEDFORD
AUTOMATIC CONCENTRATOR UNIT
AUTOMATIC CONCENTRATOR UNIT
CHAMPAIGN

Fig. 2—Teletypewriter Exchange Service—Intercity Connection Using Automatic Concentrators

A connection between two TWX subscribers, involving the use of concentrators, is illustrated in Fig. 2. In this case a subscriber in Medford, Ore., is connected to one in Champaign, Ill. Since there is little demand for local connections, and not enough business at these towns to warrant installing a TWX manually operated switchboard, they are served by automatic concentrator units which pass calls to and accept calls from some larger switching center,—in this case Portland and Chicago. Thus, a call originating at Medford is automatically passed to an operator at Portland, over one of a comparatively small group of trunks. The operator at Chicago, on learning that the call is for a station in Champaign, selects an idle trunk to that city, and picks out and rings the called station automatically by sending code combinations from her keyboard. Disconnect signals originate as soon as the subscribers turn off the power switches at the teletypewriter sets.

Actually there are about 60 TWX stations in Medford and a much smaller number in Champaign. Satisfactory service is given by the use of concentrators, with about 10 trunks between Medford and

Portland and 3 between Chicago and Champaign. Thus concentrators save line charges by eliminating individual circuits from large switching centers to distant subscribers.

TWX service includes the establishment of conference connections, in which a large number of sending and receiving stations scattered over the country may be associated together for intercommunication in typed form. It also provides service to unattended stations, with means for starting and stopping the machine motors so that messages may be left when the receiving party is absent, as well as other features of importance to customers.

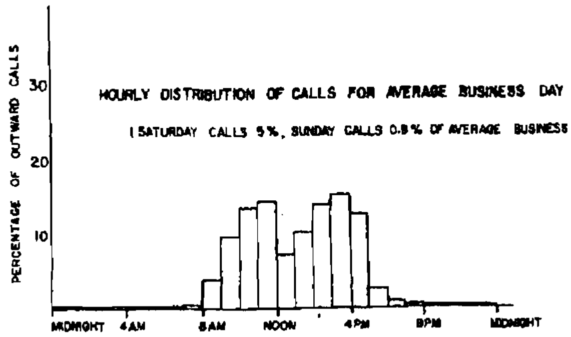


Fig. 3—TWX Outward Calls

There are now about 40,000 TWX stations in this country. The service requires several million miles of telegraph circuit facilities with about 130 manual-switching centers and 120 with concentrator units. These facilities cover the Nation, so that a TWX station may be set up at practically any point. A service of this character labors under the disadvantage that it is a business tool and follows business hours. Thus Fig. 3 shows the hourly distribution of TWX outward calls during a business day, averaged for 25 large American cities. The evening load is very light, and calls on Saturdays and Sundays are only a small percentage of those on a business day. Another disadvantage is the high cost of station equipment, which is much more expensive than a telephone set. However, since 16 or more telegraph channels can be derived from a single telephone facility, TWX toll-charges are low. Thus the toll-charge for a 3 minute TWX call is considerably less than that for a weekday person-to-person telephone connection between the same cities.

EUROPEAN AND INTERNATIONAL TELEX SERVICE

The British initiated what they called TELEX service in England not long after TWX service was started in the USA. At first a telephone subscriber was provided with a printing-telegraph machine, so that he could either talk or type over a telephone connection, provided of course that the distant party had a similar machine. The telephone switching and transmission plant was common to both services. This was contrary to the American scheme, which started and still has switching and transmission facilities for telegraphy distinct from those for telephony. Because of the large private-wire telegraph system already existing in America before TWX was started—and because tests of the operation of teletypewriters through telephone switching systems then in common use demonstrated that printing-telegraph service over these facilities would be unsatisfactory—the decision to have separate telegraph facilities for the TWX service seemed proper. As a matter of fact the British soon became aware of difficulties, and abandoned the idea of providing an alternate "talk or type" form of service through the normal telephone plant.

It is reported that the first international European TELEX connections were made in 1933 between stations in Holland, Belgium and Germany, using telephone circuits for telegraph facilities. For many years there was considerable controversy in European circles as to whether or not the International TELEX network as then foreseen should be established over telephone or telegraph facilities. After the War it was finally decided (CCIT, Brussels, 1948) to adopt the word TELEX and to use telegraph circuits. It is believed that the unsatisfactory service experienced by those countries, such as England, which tried out TELEX service as an adjunct to the telephone had much to do with this decision. However, with the introduction of toll-dialing and the provision in turn of more stable telephone circuits, it may well be that economies will be achieved by a closer association of telegraph switching with the telephone plant.

European Switching Arrangements

As might be expected, the various European telegraph administrations have adopted different switching methods for TELEX service, though a large percentage use some type of automatic method. Thus in Western Germany, which has been most active since the War in developing automatic printing-telegraph exchange service, there were over 100 automatic exchanges in use towards the end of 1954. These German exchanges employ the time-honored telephone dial, as do the systems in England, Denmark, Sweden and Finland, to enable subscribers to establish the desired connections. It is reported, however, that the automatic systems in France and the Netherlands employ the keys of the teleprinter machine to generate 5-unit switching pulses, and a paper presented at an engineering meeting in Rome last year described the TELEX system in Italy as one which also makes use of the teleprinter keyboard for generating switching signals. Manual methods are still employed in some other countries, and it is evident that with international traffic it may be difficult to establish, and properly charge for, connections which are built up on a completely automatic basis.

Rate Structure

As with toll-telephone usage, rates for TELEX service have been established on a time basis, with three minutes as the usual minimum period. However, the trend appears to be to abandon this minimum period and base the charge on the actual use of a given circuit in time-steps of five seconds each, as registered on a call meter. In general TELEX connection will cost a subscriber about half the telephone charge.

Growth

The expansion of International TELEX service since the War is shown in the following table, made up from figures for 22 countries, published in the *Telecommunications Journal*, UIT, September 1956.

Annual International TELEX Traffic in Chargeable Minutes

1946	1947	1948	1949	1950	1951	1952	1953	1954	1955
700,000	1,700,000	2,800,000	3,700,000	8,400,000	14,700,000	23,300,000	32,700,000	52,700,000	72,240,000

The above figures include service to the United States, which started in 1950 with 16,000 chargeable minutes for that year and grew to over 800,000 minutes in 1955.

TELEX Subscriber Stations

It has been difficult to obtain reliable figures for the number of world-wide TELEX subscriber stations in use today, but if the 40,000 TWX subscribers in this country are included the total cannot be far below 100,000. The number is apparently growing very rapidly, and claims are made that it increases by 10 to 20 per cent each year.

International Service with Radio Links

Since the charge for a TELEX connection is based on the duration of the call, a non-stable radio link, causing errors in the typed copy and delaying communications, is most unsatisfactory to customers. However, the development and application of error detecting and correcting codes, coupled with the provision of the necessary circuitry for eliminating from the service-charge period the delays arising from transmission difficulties, has permitted radio links to be used with success.

TELEX traffic was first handled, it is reported, over radio links in 1950, when subscribers in Holland were connected to RCA teletypewriter machines in New York. As indicated above, this transoceanic service, called TEX by RCA, has expanded greatly since that time. Though the 5-unit start-stop code is practically standard throughout the World, certain differences between the machines in this country and those in Europe had to be taken care of before this intercontinental TELEX service could be furnished. An important difference in the matter of speed. While it is usual to talk and write about a speed of 60 words per minute, neither the American nor the European machines operate exactly at this rate. Furthermore, European machines run a sufficient amount faster than American to require the introduction of a punched-tape type of automatic repeater in any inter-continental circuit connecting two of these stations.

In 1956 arrangements were completed to permit any station of the U. S. TWX network (40,000 stations) to be connected via RCA TEX service to any of the then approximately 27,000 teleprinter stations in 26 overseas countries. Since the keyboards of many of the machines of these networks are not exactly alike it was necessary to provide automatic conversion apparatus to change the form but not the meaning of certain characters. RCA reports these conversions on transatlantic calls to be as follows:

When a TWX customer transmits to a TEX teleprinter, the following conversions will be made:

$\frac{5}{8}$	will be received as	-5/8 [*]
$\frac{1}{8}$		-1/8
$		DLRS
$\frac{1}{4}$		-1/4
&		AND

[*] The dash before the fraction, as typed on European machines, is considered important to give a distinctive separation between a whole number and its fraction.

upper case H		(Trips the "Answer-Back" mechanism)
$\frac{1}{2}$		-1/2
$\frac{3}{4}$		-3/4
$\frac{7}{8}$		-7/8
$\frac{3}{8}$		-3/8
"	(Quotes)	" (2 Apostrophes)
/.	(Combined)	+? (Combined)[1]

When the overseas party is transmitting from a TEX keyboard to a TWX machine, the following conversions will be made:

?	will be received as	QUERY
:		COLON
✠		WHO R U
(		PAREN
)		PAREN
'	(Apostrophe)	, (Coma)
=		-- (2 Hyphens)
+		-/- (Hyphen, Stroke, Hyphen)
+?	(Combined)	/. (Combined)

The automatic "Answer-Back", obtained when a TWX subscriber sends upper-case H to a teleprinter, is considered an important feature of equipment used in Europe and other countries, since a machine equipped with this feature automatically transmits an identifying code-signal at the request of a calling station.

International TELEX and TEX services have become an exceedingly important phase of international communications. The basic plan was to provide a service that would appeal to customers because of low cost, reliability of transmission, and the speed with which connections would be established. The idea was to establish a sufficient number of trunks between exchanges so that even during the busy hours little or no delays would be experienced. It seems that in this case these fundamentals of a good communication service are paying dividends.

[1] This symbolizes to an overseas party that the TWX sender has completed a message and is awaiting a reply.

SECTION II—MESSAGE SWITCHING

GENERAL

The circuit switching systems considered thus far, such as TWX, TEX and TELEX, give a conversational to-and-fro type of printing telegraph service. They require the establishment of certain common arrangements before a satisfactory service of this type can be given. Telegraphy, however, has not been thought of, nor noted, for giving such an intercommunication form of service. It has been considered rather as a means of providing a record to be read, answered if necessary, and stored for future reference. Thus the sender of a telegram gave an address, wrote a signed message, and turned it over to a telegraph organization for transmission and delivery. The address routed the message through a network of circuits, and messages received at a network center would be passed manually to sending operators of other circuits. The need for incoming and outgoing circuits to operate in some common fashion was not too important.

When printing-telegraphy became common and machines for perforating tape with coded characters were available, the idea of receiving messages in perforated-tape form to be used later in the sending equipment of outgoing lines of a message center came to the fore. In this case operators read the addresses from the perforated tape to learn the proper routing. Later, machines were produced which typed the characters on the tape as well as punching them. This made the routing decision a little easier. It is apparent that a common method of working had to be adopted for these incoming and outgoing circuits. Just before and during the War a number of very large message switching centers based on manually handling tape were installed. Some are still in use. They are called "torn tape" centers, since each perforated tape message is torn from a roll of tape after reception.

In the 1920's, long before TWX service was established, it had become common practice in private-line teletypewriter service to control automatically the switching of circuits in terminal and other offices by coded impulses transmitted prior to message information. Electrical contacts associated with the mechanism in teletypewriter machines were used for switching purposes. It was not too great a step therefore to suggest that all messages in a telegraph network carry coded information which would route them through to their destinations without human aid and thus establish a fully automatic printing-telegraph message-switching system.

It is believed with considerable certainty that the first automatic switching system of this type ever installed for service was made in 1940 by the Bell System for the General Electric Company, with the message center in Schenectady. A second and larger system, with the message center in Cleveland, was put into service for the Republic Steel Corporation in 1941, just before Pearl Harbor.

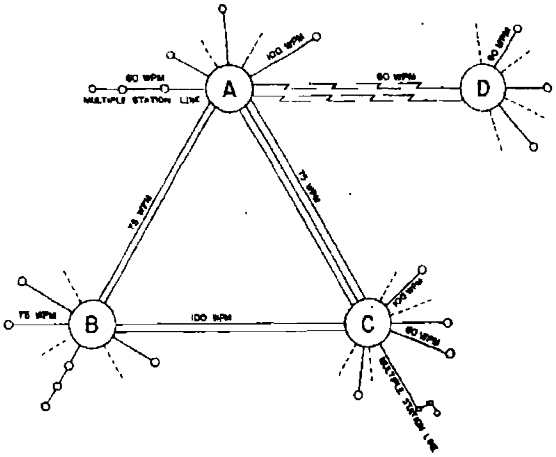


Fig. 4—Automatic Message Switching Network

Fig. 4 illustrates an automatic message-switching network, with message centers A, B, C, and D, and gives an indication of some of the complexities which arise. D enters the network via radio links, while A, B and C are tied together by land-line trunk circuits. (Many of the networks of this type are used by business houses and government agencies.) Each center may have 50 or more local circuits connecting it with sending and receiving stations. These circuits usually operate on a full duplex basis, sending and receiving simultaneously. There are three word-speeds in common use in this country today, namely 60, 75, and 100 words per minute. Since the rate charged by telephone and telegraph companies for a given circuit increases with the speed, it is the usual practice to select the most economical speed of working with due regard to the volume of traffic to be handled. Furthermore the desirability of having several stations on a line, or a "party line" type of operation, becomes apparent when in planning a network it is found that several stations are in a group several hundred miles from a center.

Over the past 15 years two general schemes for assembling and using equipment in an automatic message center have been evolved. In one, the plan of having "In" and "Out" circuits, each circuit having individual telegraph terminations, has been carried out. In the other, more use is made of shared equipment. Thus, though each incoming circuit has its individual printing-telegraph apparatus, outgoing circuits do not. On the contrary, a common bank of outgoing equipment units is provided, any one of which may, in theory, be associated with any outgoing circuit and accessible to any incoming circuit. A saving in equipment may therefore be expected. In view of different line-speeds and other matters, difficulties enter this scheme which will be touched on later.

MESSAGE FORMAT

Given that the passage of a message through a switching center must be under the control of teletypewriter characters, a simplified message format is as follows:

(1) Start-of-message characters (e. g. ZCZC)
(2) Channel and message numbers
(3) Signals to call attention to high precedence messages; e. g. Figure-shift followed by 5 J characters, 5 S characters, and letter-shift
(4) Two message-precedence characters
(5) Routing characters (routing indicators) followed by a routing-indicator termination
(6) Text of message, including address and signature
(7) End of message characters (e. g. 8 line-feeds and 4 N's)

CROSS-OFFICE OPERATION—"IN" AND "OUT" CIRCUITS

The circuits of a message center operating in accordance with the first plan outlined above and handling messages with formats similar to that just outlined are shown schematically in Fig. 5, while Fig. 6 is a photograph of such a center. Incoming lines in Fig. 5 are at the left, outgoing at the right. Each incoming message is recorded in punched as well as typed form by a typing-reperforator machine. Each such recorded message is read by machines marked T in the diagram. In some installations these devices will read or sense the last character of a given message in the received tape, though this character is closely

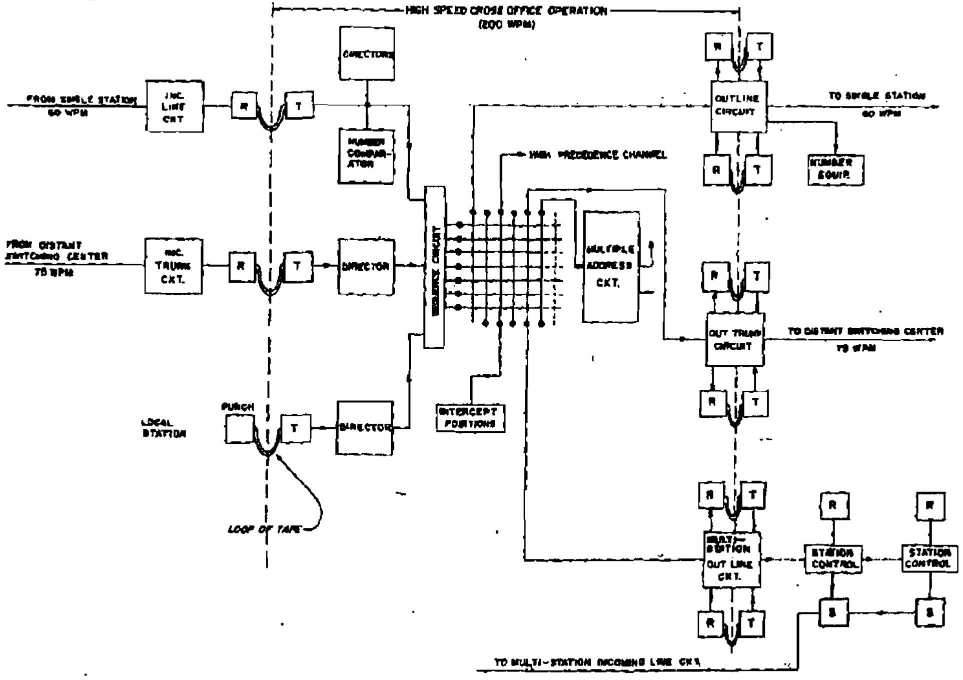
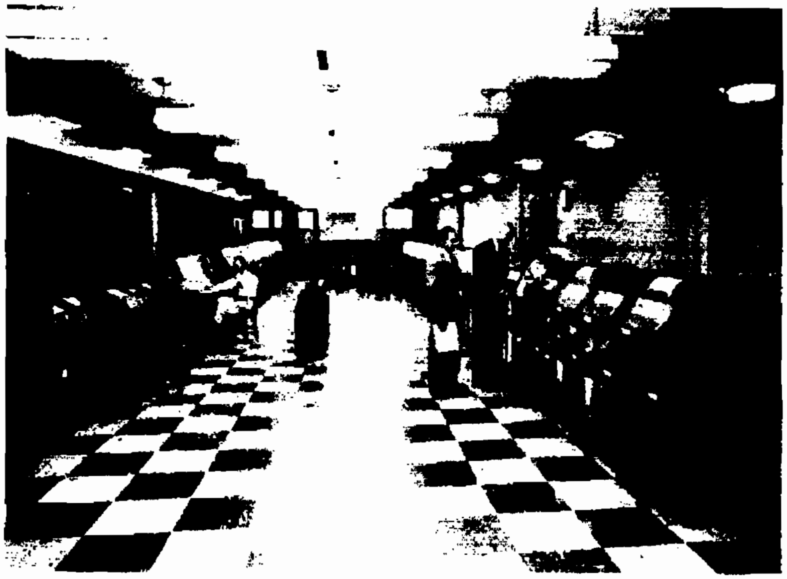


Fig. 5—Message Switching Center.
Cross-Office Operation From Incoming Lines to Outgoing Circuits



(Courtesy of the American Telephone and Telegraph Co.)

Fig. 6—Message Switching Center.

adjacent to the punches of the perforating mechanism. In others it is necessary to "feed out" several inches of tape to permit the last message character to be sensed. Immediately following the receipt of the start-of-message (SOM) characters it is a fairly common, though not a universal, practice to check the channel and message numbers to make certain that a proper message-numbering sequence is being followed.

As noted below, it is a military custom to have six message-precedence classes, but in the transfer of messages from "In" to "Out" lines in the message-center it is now the practice to divide messages into two precedence classes: high and low. The arrival of a high-precedence message at a center causes alarms to be given to alert the attendants. The precedence characters which control switching operations follow. The routing characters will usually consist of several characters for each addressee, and for several addressees these may add up to 50 or more, terminated by a special group. The text of the message, with the address and signature, follow in a routine manner, to be ended by a special end-of-message (EOM) character group which prepares the equipment for the next message.

Incoming line-readers (marked T) read one character at a time, and it is apparent that several characters have to be sensed before a decision as to the next procedure can be made. Thus information must be stored and used later. Telephone-type relays have been used for this purpose, and directing-equipment and sequence-circuits may be assemblies of relays and switches. The objective is to connect the transmitter associated with the reader of an incoming line circuit with a recorder-reperforator associated with the proper outgoing line or trunk. As soon as routing information is analyzed, the director controls switching operations to make this connection through some type of mesh or grid as illustrated, or by other means. Once this path is established the message is transmitted across the office to one of two receivers, whichever is idle at the moment, associated with an outgoing circuit; two are installed to prevent traffic delays. The speed for cross-office traffic in recently established centers is 200 words per minute, but it is apparent that the rate at which a given message leaves a center is not determined by the cross-office speed but by the speed of the outgoing line to which it is sent. As indicated, the receivers of outgoing circuits pass perforated tapes to transmitters, which operate alternately for fast traffic handling.

PRECEDENCE TRAFFIC

Automatic message-switching systems can readily handle precedence traffic. In the Military installations now taking form messages will have six degrees of precedence. These, with their character designations, are Flash (ZZ), Emergency (YY), Operational Immediate (OO), Priority (PP), Routine (RR) and Deferred (MM). However, as mentioned above, for cross-office operation in the switching center only two classes, High and Low, may be recognized. In some instances the three top precedence designations of the above list will be rated High, the others Low. On the other hand, when messages are transmitted on outgoing circuits all six degrees of precedence, as well as the time that any given message has been in the office, may be considered to determine the order in which the messages will be sent out.

Since there are at least three different engineering groups in this country developing telegraph message-switching systems, variations in the general plan are bound to occur, and this has been true as regards the handling of precedence messages. In some installations a message of low precedence is not transmitted across the switching office until it is fully received. A high-precedence message, however, cannot suffer such a delay, and is started across the office as soon as the director, operating from the routing indicators, switches the message to the proper outgoing line or to a special high-precedence channel. In another plan all messages are started across the office as soon as the routing determinations have been made.

Again, different plans are followed for handling precedence messages at the outgoing line terminations. In one case the action taken on the arrival of a high-precedence message at an out-terminal then handling a message of low precedence is to interrupt this message and insert the other in its place. An alarm indicates that such action has been taken, and an attendant later puts the interrupted message back into the system. According to another method no message is interrupted, but the high-precedence message seizes the line ahead of any waiting message of lower grade as soon as the line is free.

MULTIPLE-CALL MESSAGES

A message to a large number of addresses will be handled by an automatic switching center if the routing indicators for each addressee are properly inserted in the format. The director and other equipment handling a given multiple-call or address message has the problem of assembling all the necessary outlets as designated by the routing indicators, so that when the message is forwarded from a transmitter all addressees will receive a copy. The equipment and circuit arrangements provided by the different development organizations to meet the requirements for handling multiple-address messages differ quite radically.

MULTIPLE STATION LINES

Mention has been made of the desirability of providing several stations on a given line to save line costs. In some instances as many as 10 stations on a line may be provided, but the difficulties involved in handling traffic to and from lines with as few as three stations will be evident from a consideration of Fig. 7. This shows a three-station line being operated full duplex (i. e., with simultaneous operation of send and receive channels) with sending and receiving equipment at each station. It is evident that only one message at a time can be

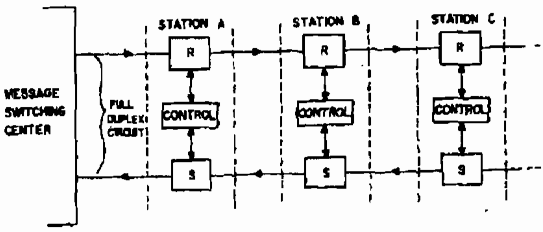


Fig. 7—Multiple Station Line

received at either A, B, or C. Furthermore if a message is destined for C only, receivers at A and B should be inactive—actually locked out.

As regards sending, it is also clear that when one station is operating; the others cannot. Furthermore, if the traffic load is approximately uniform it is desirable to prevent one station from unduly holding the circuit. Signals may therefore be automatically transmitted from the center to start transmitters at station in rotation. A station without traffic—no tape in its transmitter—will be passed, and the next station tested for traffic.

INTERCEPT OPERATION

Differences in operating periods because of time zones, holidays and other factors bring about the need for the interception of messages at switching centers and transmission to addressees at later times. Thus a director may be so arranged that any message with a particular routing indicator will be sent to an intercept station in the center. Furthermore, any message with an unassigned routing indicator will be automatically transferred to intercept, and alarms sounded.

AUTOMATIC NUMBERING AND TIMING OF MESSAGES

The usual requirement is that all messages leaving a center are numbered and timed automatically, which means that the normal flow of characters is interrupted while symbols conveying this information are inserted.

CROSS-OFFICE OPERATION—POOLED EQUIPMENT

Fig. 8 diagrams sketchily an office of this type. Incoming lines each with typing reperforators, tape transmitters, relay banks and other apparatus are at the left, while outgoing lines with numbering and timing machines are at the right. For each group of about 25 incoming lines there is one common director with an associated translator. This relationship depends on the type and number of messages to be handled in a given busy period.

Each of the common cross-office units has a reperforator for receiving from incoming line units and a tape transmitter for sending to outgoing lines. Of course arrangements to meet all the different traffic situations must be provided. If all lines were operated at the same speed and no other variations, such as single and multiple station lines, were encountered, it is evident that *any* non-busy cross-office unit would be accessible to *any* incoming line and transmit in turn to *any* non-busy outgoing circuit. Thus a pool of cross-office units is available on call, and the plan appears economical when compared with the first scheme, in which *each* outgoing line has its own teletypewriter terminal equipment.

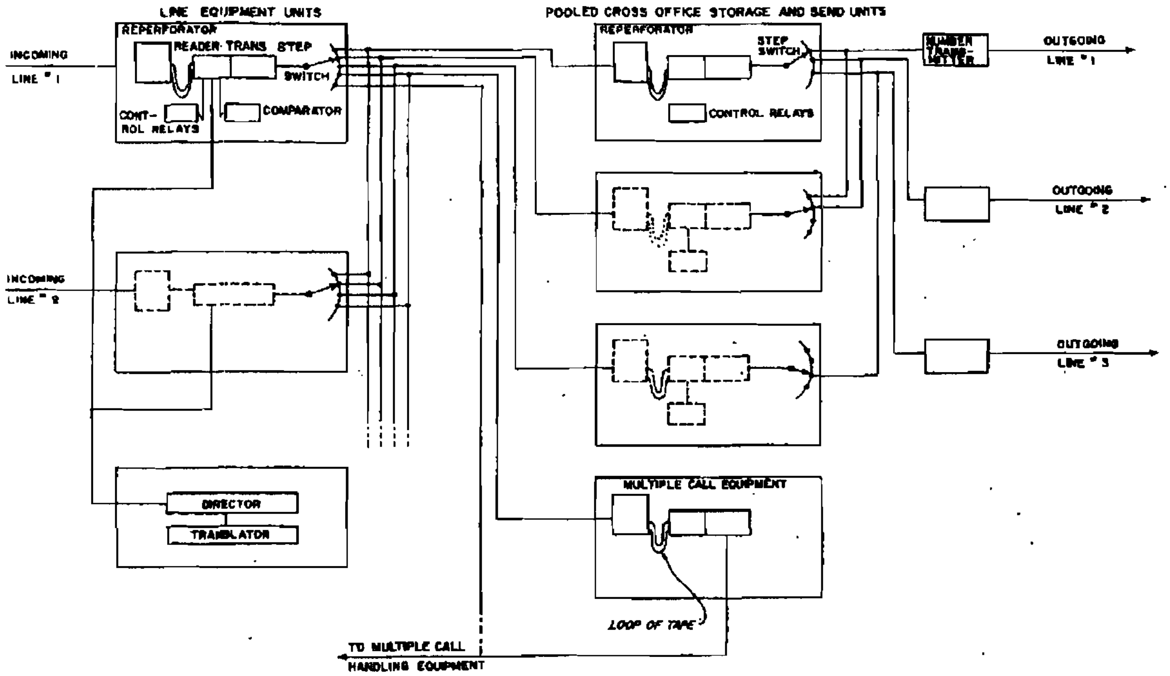


Fig. 8— Message Switching Center. Cross Office Operation Using Pooled Equipment

Complexities arise however when lines of different word speeds terminate in the same office, and an equipment pool is required for each speed.

The Army is proceeding with its network on the basis of pooled apparatus, while the Navy and the Air Force have equipment based on the other scheme. It will be some time before the relative merits of the two arrangements will be completely thrashed out.

TRUNKING CIRCUIT DETERMINATIONS

The number of trunks needed between two switching-centers to provide satisfactory service, bearing in mind the economics of a given situation, becomes a problem in probability. The quality of service to be given, i. e. the amount of allowable message delay, must be considered in connection with busy-hour loads, length of messages, cost of trunks and other factors. In some message-switching systems practically all messages are short, so that routing indicators and the like constitute a fairly large percentage of the message. Also many of these short messages—e. g. air traffic control messages—must be delivered very quickly or their value is lost. These and other considerations have a bearing on the determination of the number of trunks to provide for a particular case.

SECURITY WITH MESSAGE SWITCHING SYSTEMS

It is evident that characters used for switching purposes must enter a switching office in the clear. Also, if traffic-flow security is to be achieved, these characters must *not* be in the clear on lines between centers and from outlying stations to centers. To meet these two requirements all such circuits will have to be furnished with cipher equipment on a center-to-center and station-to-center basis, giving what has been called "link encipherment". The body of a message will be in the clear while it is passing through the switching office, unless the message has been doubly enciphered.

CONCLUSION

It seems evident that while message-switching systems are economical of plant facilities and especially of long distance circuits, they introduce a host of other problems in that they must handle different types of messages with a variety of precedence values and at different speeds. If long circuits needed for printing-telegraphy were plentiful and cheap it would seem that the direct-circuit method of switching would be preferable. Here the problem of handling various types of messages falls back on the user of the service, and the switching system rids itself of that burden. Moreover, users with direct connections between their

terminals should receive better over-all service than those who depend on having their messages handled by a second party, even though that party is an automatic mechanism.

It is believed that the great expansion of telephone service which has occurred when trunking circuits and other facilities are provided on a liberal basis to give virtually a no-delay service is an indication of what could happen to "printing-telegraphy" if connections between teletypewriter stations anywhere in the world could be established in a similar fashion.

Appreciation is expressed for the work of those who very kindly read the draft of this paper and offered their comments.

Chatter Patterns: A Last Resort

BY W. E. STOFFEL

Unclassified

A possible method of identifying radio operators by their reaction to standard situations occurring in chatter, for use when conventional techniques fail.

BACKGROUND

The success or failure of most traffic analysis problems depends primarily upon the analyst's ability to achieve continuity.[1] Simply defined, continuity involves bridging a communications change by equating a given element appearing before the change with a different element appearing after it. The term continuity refers to the discovered relationship between the given element and its replacement, *without reference to the underlying meaning.* For example, we may by various methods discover that callsign ABC during November was replaced by DEF during December, and thus achieve continuity from ABC (November) to DEF (December). Note that the time factor is intimately involved in the relationship, since DEF replaced ABC. If, for example, ABC in November was found to be the same transmitter as GHI in November, the relationship between ABC and GHI is more accurately termed an equation or co-location and is not a continuity in its pure sense. Continuity can exist between ABC and DEF without any knowledge of the location, identity or function of ABC or DEF. The importance of the distinction between continuity and other forms of equation lies in the fact that once any knowledge is gained about ABC, *it automatically applies to DEF* (and vice versa). If we discover that

[1] A number of countries today go to surprising lengths to suppress in their communications systems distinctive characteristics which might serve to disclose their identity. Among the more common methods of suppressing characteristics is that of frequently changing certain communication elements, such as callsigns, frequencies, schedules, procedure, routing and address symbols. Since it is often necessary for the traffic analyst to study several months of material on a given net before concrete intelligence results can be developed, and since communications elements may change as often as twice each day, he must, somehow, find a way to nullify the effect of these frequent changes in order to pull homogeneous material together for study. He may note certain characteristics which do not change frequently (as, for instance that a given station sends a distinctive service message each day at 1100), which can serve as identifying features. When he is successful in nullifying a communications change, the traffic analyst refers to the result as *continuity.*

ABC served the Chief of Staff, 12th Division, Greenville, for his contacts with subordinate regiments on the Division administrative/logistic net, this information applies to DEF, in toto. On the other hand, about GHI we can only say (with any certainty) that it is located at Greenville. (Depending upon the type of equation made between ABC and GHI, we may further be able to say that GHI also serves 12th Division, or that it also serves an administrative/logistic function).

A direct cryptanalytic analogy to continuity can be recognized by considering a simple substitution system involving a matrix with changing coordinates. For example, the following matrix has been recovered for 1 April:

$$\begin{array}{c|ccccccc}
 & 4 & 2 & 1 & 8 & . & . & . \\
\hline
2 & A & D & R & L & . & . & . \\
9 & P & B & O & C & & & \\
3 & M & - & E & T & & & \\
1 & - & K & N & - & & & \\
. & . & & & & & & \\
. & . & & & & & & \\
. & . & & & & & &
\end{array}$$

On 2 April, assumption of the probable word "ATTACK" yields:

47	23	23	47	63	55
A	T	T	A	C	K

$$\begin{array}{c|ccccccc}
 & 7 & 5 & - & 3 & - & - & - \\
\hline
4 & A & D & R & L & . & . & . \\
6 & P & B & O & C & & & \\
2 & M & - & E & T & & & \\
5 & - & K & N & - & & & \\
. & . & & & & & & \\
. & . & & & & & & \\
. & . & & & & & &
\end{array}$$

It can then be stated, if the assumed word "ATTACK" proves correct, that row coordinate 4 on 2 April *is continuity of* row coordinate 2 on 1 April. It can also be shown that cipher value 57 on 2 April *is continuity of* cipher value 14 on 1 April. In this second case, we have achieved continuity without knowing what the actual plain value is. Finally, we can say that cipher value 43 on 2 April is continuity of cipher value 28 on 1 April. In this instance when 43_c (2 April) = 28_c (1 April) is proved, and 28_c (1 April) = L_p, then 43_c (2 April) = L_p.

The more frequently an element changes, the more important continuity becomes (since it is virtually the only consistent method for achieving enough depth on a given element so that a study of its underlying nature and purpose can be undertaken), and the harder it is to get. Most of us can sympathize with the unfortunate analyst whose formerly stable problem suddenly adopts twice-daily changing callsigns, frequencies, addresses and discriminants.[1]

On problems involving fast-changing elements, continuity is usually achieved by means of whatever characteristics are available that can be trusted to be unique. If many are available, the easiest, fastest or most economical methods are, of course, tried first, while the more intricate and time-consuming methods are held in reserve for tough cases. It often happens that certain nets develop a stubborn streak which defies description (in mixed company) and, despite application of the most time-consuming routines, manage to remain intact and featureless.[2] Where all else has failed, the analyst may well find the following proposed routine useful.

INTRODUCTION

Most people are creatures of habit, particularly when performing a routine task, and radio operators are no exception. There has been considerable experimentation with and study of the variable characteristics of a Morse operator's transmitting habits or "fist" in an effort to develop a systematic process of recording and analysis which would permit ready recognition of the individual at the key. There is, however, a large area of variable operator habit which has remained virtually unexplored during recent years: habitual operator characteristics as displayed in routine chatter exchanges.

A good many traffic analysts can recall a specific instance where a unique or rare procedure signal was consistently used by a certain net or station and, in the last resort, could thus be relied upon to identify its user. There may be few, however, who can recall conducting a comprehensive and systematic search for such characteristics in order to achieve continuity and identification.

What follows is an outline proposal for a routine of systematic search for unique chatter or conversation characteristics which can be used for

[1] Traffic analysts will recognize that, for the sake of simplicity, the complexities of the various classes of equations and their accompanying validities have been avoided in this presentation. Other readers are warned that many a "Donnybrook" can and does develop between traffic analysts on these very factors.

[2] This situation tends to exist to a greater or lesser degree on most problems, although it can be appreciated that the point is ordinarily glossed over in discussion unless the words "additional personnel" are injected into the conversation at a suitable point.

continuity or co-location purposes. For the most part, specific details are avoided, except for examples, since they will vary from problem to problem. It will be seen that the routine is not readily usable on large problems, and may, in fact, be suitable only on limited problems where the area of inquiry is relatively small and all standard methods of achieving continuity have failed. An obvious prerequisite would be a significant volume of activity transmitted by the stations under study, with some assurance that a fairly complete (preferably verbatim) copy of chatter has been recorded by the intercept operator.

BASIC ASSUMPTIONS

It can be empirically demonstrated that regardless of the degree of conformity enforced by the target's COMSEC service, different operators use different combinations of procedure signals to express the same ideas, but that each operator tends to be consistent with himself.

The writer's contention is that these habits are more widespread than is generally supposed and that, under admittedly special circumstances, a *systematic routine* will disclose a sufficient number of them to permit continuity to be developed.

Expert chatter readers will recognize that operator chatter must be treated as a distinct, albeit peculiar, language.[4] Despite the best intentions of the signal officer who compiles an extensive set of procedure signals for radio operations, the "plain" side of his "code" is generally restrictive in nature. In actual operational use, a given procedure signal (prosign) tends to lose its rigidity and takes on a more general *concept* or *idea* form (particularly where it is used so often as to be easily recognized without "looking it up"). Thus the prosign QTR can be shown to have the fixed meaning "The correct time is ____ hours", whereas in actual usage among experienced operators, it embodies the general concept of *time* and is so used in a wide variety of contexts.[5] Complementing the tendency of experienced operators to generalize prosign meanings is the equally strong tendency to minimize and abbreviate words and prosigns in order to conserve both time and energy. "Ham" chatter displays this quite clearly.[6] It is not difficult to visualize how a relatively isolated segment of a radio network could gradually evolve a "local dialect" distinct from that of the rest as a result of improvisation under these pressures. Certainly a regimented COMSEC system with a firm domination over the radio schools could suppress some of this variation, but if we confine ourselves to studying experienced operators, it is likely that some recognizable variance and individuality will occur.

A SAMPLE PROBLEM

If distinctive operator habits do, in fact, exist, how do we go about finding and recording them? Evidently, if a way can be found to catalogue the *situations* that confront a radio operator most frequently, we can collect his *responses* to any given recurring situation and by observation determine whether his reaction is fixed by habit or is variable. For example, we might select as a favorable starting point several hours of intercept between station A and station B during which a number of messages were sent by each station. As a recurring situation, we might select *message transmission*, and further restrict our examination to the station responses during the period immediately before starting each message. We might find:

Example 1

A:	QTC	(I have traffic for you.)
B:	GA	(Go ahead.)
A:	C AS	(Yes, stand by.)
B:	C	(Yes.)
A:	BT	(Break Sign—attention, etc.)
A:	NR	(Goes into preamble.)

Examination of the same basic situation a short time later when station A was again about to transmit a message showed that after receiving "GA", station A *again* said "C AS" (Yes, stand by) and after receiving the affirmative from the other end began his transmission with a break sign. A third message still later in the same schedule begins with the same exchange and it now begins to look as if we have found a starting point.

A quick look at the activity of station B shows that the two messages it sent were also preceded by identical chatter exchanges:

[4] A more precise analogy has been suggested which compares chatter to a code book usage wherein (a) the vocabulary is not precisely suited to the material being encoded, and (b) the code is large enough so that code-clerks tend to use combinations of common, memorized groups in preference to rarer but more precise and economical groups which must be looked up each time they are needed.

[5] For example, the interrogative form "QTR?" is listed as "What is the correct *time?*" The prosign QSY *means* "I shall send on ——— kilocycles" and its interrogative form (QSY?) is interpreted as "On what frequency should I send?" or "Should I change frequency?" The compound "QTR QSY?" may well be used to mean "When should I change frequency?"

[6] For example, the prosign "CUL" is a "Ham" contraction of "See or contact you later."

Example 2

B:	QTC AAA	(I have an "AAA"[7] message for you)
A:	AS	(Stand by)
B:	C	(Yes)
A:	GA	(Go ahead)
B:	C AS	(Yes. Stand by)
A:	C AS	(Yes. I'll stand by)
B:	C (pause) BT	(Yes. Break sign—attention)
		(then into preamble)

Let us now examine what we have so far in the way of possible habits:

(a) When *offering* a "QTC," both station A (Example 1) and station B (Example 2) sent "C AS" *after* receiving "GA" from the other end. Each then preceded the preamble with "BT," but station B (Example 2) used the compound "C (pause) BT."

(b) When *receiving* a "QTC," station A (Example 2) responded with "AS" before giving the "GA," while station B (Example 1) gave "GA" immediately. When responding to "C AS," station B (Example 1) gave the brief answer "C," while station A (Example 2) used what may be a variant form—"C AS."

Later the same day, another exchange of messages is found between stations A and B. During this later schedule, two messages from station A are preceded by:

Example 3

A: QTC
B: GA
A: C (pause) VVV QTC
(goes into preamble).

and one message from station B is preceded by:

Example 4

B: QTC
A: GA
B: C AS
A: C
B: C (pause) BT
(goes into preamble).

[7] "AAA" in this instance refers to type or priority of message (e. g., "2nd priority" or "service").

It is quickly seen that the behaviour of station B is essentially unchanged, but that of station A shows no parallel with what went before. Our choice at this point is quite simple—either station A has changed operators or the "habit" is not sufficiently strong. The resourceful analyst would study carefully the chatter exchange during the opening of this second schedule for any evidence of a new operator at station A (extensive tuning, authentication, etc). If the "new operator" hypothesis does not appear sound, other types of habit must be sought. On the other hand, if it *does* appear sound, examination of suspected continuities from previous or successive dates should show whether *the time of change is fixed (i. e.,* the end of one duty tour and the beginning of another). It would appear that once the duration and change times of operator shifts can be established, analysis can proceed at a much faster rate, since the change times will allow the analyst to sort activity for any given date into tentatively homogeneous groups.[8]

Thus far, our accumulated results are far from impressive. Where can we look for other habits? Two situations obviously related to the one examined above would be the area immediately following the message (message closure and receipting exchanges) and any "in-text" servicing (receiving station interrupting to ask for repeats while the message is still being transmitted) or "post-text" servicing (after the message is finished but before receipt is acknowledged), but there must surely be other areas which could be equally profitable.

TYPICAL SITUATIONS

We may find it useful to consider a typical schedule between two stations and examine the successive *situations which confront* the radio operator. Since certain of these will tend to recur within the same schedule (e. g., opening traffic, as in the example above), while others by their very nature, will tend to occur only once in any given schedule, it is convenient to distinguish between the two types, since the former is much more *useful* as a starting point (one is bothered less by possible operator changes, and only one schedule is generally needed for initial isolation of a tentative habit) while the latter comes into use, for the most part, after some initial foothold has been achieved. For purposes of convenience, we shall call the former *primary* and the latter *secondary habits.*

[8] Some care must still be exercised in watching for cases where extra operators are put on to cope with heavy traffic volumes, or for any other situation having the same effect.

1. Call-Up and Initial Contact

A surprising percentage of nets do not achieve immediate, or nearly immediate, contact, and extensive calling is therefore found frequently enough to be considered a regular source of habits. The calling operator (sometimes both ends are allowed to call) will often develop a fairly long and stylized *calling sequence* which is composed of several distinct elements. For example, one popular sequence appears thus:

Example 5

```
VVVVV  ABC ABC ABC ABC DE DEF DEF
VVVV   ABC ABC ABC ABC DE DEF DEF
VVVVVV ABC ABC ABC ABC DE DEF DEF QTC QSA?[9] R K
```

The calling operator may then pause, waiting for a response from ABC, and if none is forthcoming, repeat the full sequence and pause again. For purposes of convenience we may arbitrarily label the component elements of the calling sequence thus:

Tuning (V's)
Main Call (ABC . . . . DE DEF . . . .)
Closure (QTC . . . . . K)

The actual tuning character or characters are normally fixed by the signal officer, but the *number* of repetitions sent may be useful—unfortunately, however, few intercept operators can be relied upon for verbatim recording of a long and uninteresting series of V's. The only useful feature of the main call (in this example) is the *number* of times each callsign is sent. Empirical evidence suggests that this feature is usually fixed by the signal officer, and when it is not so specified it may be too variable to be useful as a habit. Likewise the *number* of main calls used in a calling sequence is usually specified by the signal officer, but where departures from specified practice are found, they may constitute reliable habits. But by far the most useful element of the calling sequence is the closure. A wide variety of prosign compounds are used here, and they tend to be habitual. The first response of the station being called is also a likely source of secondary habits, as is the first station's reaction to this response. At a minimum, signal strengths and readabilities are exchanged at this time. It is common practice for some nets to use callsigns only when making initial contact, for both brevity and security purposes, and under such circumstances, the point at which callsigns are consistently abandoned is sometimes useful.

[9] QSA?—"What is the strength of my signals?"

2. Tuning

Immediately after initial contact, various adjustments of tone, power, and frequency must usually be made before reception is considered good enough for the transaction of business. The exchanges may range from a short, terse and businesslike operation to a long, temperamental and often humorous argument. Unless they occur frequently, these longer-winded battles are of little use to the type of study being described,[10] and attention should be concentrated upon the shorter and more lucrative exchanges.[11] The first schedule after a frequency change usually contains much more tuning chatter than do subsequent schedules on that same frequency.

3. Recognition

Recognition exchanges may occur with or without a specific system such as an authentication chart or table of challenges and responses. They are most often seen on the first schedule after a new operator comes on duty, although some signal plans seem not to require their use unless messages are to be exchanged, while others obviously specify such use on every schedule. Many experienced operators prefer to rely on aural recognition of "fist" characteristics and frequently ask the other end to "send V's" (QSV) or adopt some other device toward the same end.[12]

4. Opening Traffic

The exchanges treated in some detail (see *Examples 1–4*) may be preceded by statements from *both* operators that they have traffic to be transmitted. In this situation, agreement must be reached on an order of transmission and such an exchange may be a good source of secondary habits.

5. Preamble and Text Handling

This category embraces a wide variety of characteristics, some of

[10] Except, of course, for the laudable purpose of recreation.

[11] In analyzing these exchanges, it is useful to remember that frequently the operator at the key does not have direct access to the transmitter itself and must relay adjusting instructions to a remote transmitter site by telephone.

[12] This use of QSV should not be confused with the more extensive use during tuning or equipment adjustments. When the sending occurs early in the schedule, it is not always easy to distinguish between the two, but its use in the recognition sense is usually unmistakable when, during later operations, consistent mis-encipherment of procedure, etc., arouses clearly recognizable operator suspicions about an operator's identity.

which are generally recognized as useful. In order to find *operator* habits, rather than *station* habits, one must recognize that the operator is here working from a printed or written record, so that the order of preamble elements, for example, is controlled (in most problems), by their arrangement on the message form while breaks and separators may generally be attributed to the operator himself. Here also belongs the situation where the operator realizes he has mis-sent a portion of the text, sends an error sign, and corrects the mistake. In this category, one is most definitely at the mercy of the intercept operator and one is likely to find him completely absorbed in copying the text (to the exclusion of non-textual transmissions).

6. "Break-In" Servicing

The receiving operator, under certain signal instructions, is allowed to "break-in" during text transmission to ask for verification or repeats of certain passages which he has missed or which seem doubtful. Where this happens (and where the intercept operator provides a verbatim record of the exchanges), primary characteristics may be found, since a number of prosigns are usually available for use in this situation, and requests for repeats can and do take several forms.

7. Closing Traffic

Most signal instructions will provide for some prosign such as BT, BK or K to mark the end of text, but some operators use additional compounds for emphasis, or to remind the other end that there are still more messages to be transmitted. As a special case, traffic sent by broadcast methods is usually sent twice, and the procedure used to separate the two consecutive transmissions frequently shows strong habit patterns.

8. Post-Message Servicing and Receipting

From the transmitting operator's point of view, a given message has not been "cleared" until the other end officially receipts for it. If the other end is not satisfied that his "copy" is correct, he will not give a receipt (QSL) until he has verified the questionable passages. Although the situation is slightly different from that described above ("Break-in Servicing"), habits found in one situation would be likely to show up in the other. As a special case, servicing may be asked for during a later schedule and, if it can be shown that the message has already been "cleared" (i. e., that a QSL was given), this "late" servicing may well result from an inability to decrypt the message.[13]

[13] Such information might be particularly useful to the cryptanalyst.

The servicing request in this instance may differ from "break-in" or "post-message" servicing only to the extent that the involved message must be clearly identified (i. e., by serial number or other unique indicator).

9. Breaks, Waits and Interruptions

We are here concerned, not with pauses which appear to be a fixed part of habits rising out of other situations (i. e., the pause before message transmission as shown in the first examples above), but rather with the non-routine or unexpected interruptions which cause temporary or permanent breaks in a given schedule. Among the situations which can be expected to produce habitual responses[14] are intervention of other schedules, equipment failures, interference, operator changes, shortage of transmitters and interruptions by other stations.

On especially long waits, the transmitting operator may key certain characters or compounds to "hold" the other end, in the general sense of "Hang on, I'm still here" or "Keep listening, I'll only be another minute or so." The actual signals sent during this "hold keying" may well be unique to each operator, but again we are dependent upon verbatim intercept copy if this characteristic is to be used.

10. Next-Appearance Discussions

Once the business of a given schedule has been transacted and the schedule is about to be terminated, some mention is usually made of the next appearance. Where contact times and frequencies are predetermined by the signal instructions, this mention is not likely to exceed a very perfunctory "Watch for me; I'll watch for you." On the other hand, the discussions may well involve times and frequencies. Either situation will yield useful secondary habits. As a special case, satisfactory contact may not have been achieved and ensuing discussions about another time and frequency may yield significant habits if the situation recurs.

11. Sign-Off

The actual termination of a schedule frequently involves a little ritual which is difficult to describe to one who has never heard it. Between operators who are used to working with each other it is

[14] Obviously, interruptions caused by flood, fire and other emergencies cannot be expected to appear often enough to be a fruitful source of habitual responses.

usually fairly rapid and highly stylized.[13] While this area should not be ignored as a source of habits, a departure from the routine specified in the signal instructions is frequently th? result of tacit agreement between *both* operators and must be treated accordingly.

12. Special Circumstances

The above categories obviously do not complete the list of situations which may be useful on any given problem. If the net under examination regularly changes frequencies in mid-schedule, the chatter exchanges before and after each change merit some observation. Another special case involves the use of a matrix or table for prosign encipherment. Aside from the obvious benefits such a system can provide where local usage makes it effective for net or complex identification, the *use* of each *cell* in the matrix can be likened to the use of a comparable *prosign*. Thus, habitual use of certain cells or the formation of various compounds is just as useful as the prosigns themselves. This principle also applies to related systems, such as authentication, wherever habits can form as a result of allowing the operator a free choice in selection among a number of variables.

CONCLUSIONS

It will be evident that the proposed approach to maintaining continuity through chatter analysis has application only in limited cases. Because of its complexity, it may well be attempted only as a last resort and would undoubtedly require the services of a skilled chatter reader.

On some problems, one or two distinctive habits may be sufficient, while on others a wide variety of situations may need to be examined before individual operators can be distinguished. It may be found useful, when looking for habits, to keep a similar running record of those responses *which are the same for all operators*, on the theory that such responses have been specified by the signal instructions or form a "local dialect." Such a list would be helpful in later examinations of a related net or complex, since it would define situations where habits are *not* likely to be found. (It might also become a useful *net identification* tool.)

It should be emphasized that the "habits" we seek in this approach are not *tendencies* to act in a given manner, but are more nearly *instinctive* reactions or reflexes to recurrent stimuli. Where these reactions are found to be quite variable, it may be assumed that the operator concerned lacks sufficient experience to have developed such habits, or that the situation is rare enough so that he has not developed a reflexive response.

The approach may be useful, not only for continuity development in selected areas, but for inter-net equations after other evidence has narrowed the area of search to reasonable proportions, and to bridge communications changes where continuity is available both before and after, but not across, the change.

[13] A typical exchange sometimes used by U. S. personnel, where conformity to COMSEC regulations is not rigidly enforced, involves the transmission EF (dit, di-di-dab-dit) and the answer EE (dit, dit), which approximates the rhythm of the familiar "Shave and a haircut . . ."

Introduction to Traffic Analysis[1]

BY LAMBROS D. CALLIMAHOS

~~Confidential~~

A basic exposition of the principles and techniques of traffic analysis.

GENERAL

Traffic analysis is defined as that branch of cryptology which deals with the study of the external characteristics of signal communications and related materials for the purpose of obtaining information concerning the organization and operation of a communication system. By means of traffic analysis valuable information can be derived concerning the enemy and his intentions, even without actually reading the texts of the intercepted messages; the solution and translation of messages are the functions of cryptanalysis and not traffic analysis.

Traffic analysis can yield a detailed knowledge and thorough understanding of a communications network; traffic analysis techniques involve, among others, the reconstruction of the nets and the determination of the methods of their operation, the solution of callsign and routing or address systems, the solution of frequency rotation systems, the identification and analysis of components of the message externals, the interpretation of radio procedure, the study of the distribution of cryptosystems, and the analysis of authentication systems. The results obtained from traffic analysis materially contribute to the following:

Intercept operations. Traffic analysis provides information such as call signs, frequencies, locations, and schedules pertaining to target enemy stations, thus assisting intercept stations in the accomplishment of their missions; and, in coordination with cryptanalytic and intelligence interests, traffic analysis assists in establishing the priorities for the interception of individual circuits.

Cryptanalysis. Traffic analysis furnishes assistance to cryptanalysis in many ways, depending upon the particular communications situation; this assistance includes information as to the identity and location of radio stations, information of cryptanalytic interest gleaned from enemy operators' "chatter," identification of possible stereotype or proforma messages from external characteristics of the traffic, and identification of isologs.

[1] This article is an extract from the forthcoming NSA text, *Military Cryptanalytics, Part II*.—Editor

Intelligence. The organization of a radio network and the manner in which messages are passed over this network reflect troop disposition, command relationships, and impending movements and preparations for military activity; therefore an analysis of net structure, traffic contacts and patterns, traffic volumes, and similar communications features, is of considerable assistance in building up a complete intelligence picture.

Security. The techniques developed by traffic analysis in the attack on intercepted enemy communications may also be applied to our own monitored signal communications in order to uncover possible weaknesses and to maintain high standards of communication security by preventing these weaknesses from developing in our communications.

There are three kinds of basic data used in traffic analysis as follows:

Intercept data, comprising all information supplied by the intercept operator, and consisting of the frequencies on which transmissions are heard, the time the transmissions are heard, intercept operator comments such as signal strength and audibility, "fist" characteristics of the target radio operator, and any peculiarities in the transmission or handling of the traffic that strike the intercept operator as being significant or out of the ordinary.

The transmission, comprising everything transmitted by the target radio operator, and including the initial call-up, the exchange of call signs, the traffic passed, the servicing incidental to the traffic being passed, the radio operators' chatter, and the signing off. Traffic consists of the message externals (i. e., the preamble and postamble, if any) and the message text proper. The externals comprise various items that facilitate the handling of the message, among which are the radio station number and perhaps a message center number or other reference numbers, the group count, routing and address information, precedence indicators, the file date and time, etc.; all this information is of considerable potential value in traffic analysis. The message text, if it displays patent cryptographic characteristics, can also be of use.

Collateral information, comprising any information, other than that derived from a study of intercepted communications, which may be of value in traffic analysis; e. g., captured documents, intelligence reports, etc. In addition, traffic analysis is aided by *communication intelligence collateral* such as direction-finding bearings, Morse operator analysis, plain language messages, and decrypted traffic.

In traffic analysis the details of each feature of the communications operations or structure are studied, followed by analysis of the interrelationships among these features, culminating in the reconstruction of an entire net together with all the details of its operation. At the start of a traffic analysis problem, little may be known concerning the target communications; it would first be necessary to segregate initially intercepted traffic into several major types or nets by means of cryptographic features, common operating characteristics, or other means. At this point the intercept stations are given general search missions over the entire range of radio frequencies to intercept desired types of transmissions. As traffic accumulates, fragmentary nets are diagrammed and analysis is begun on the transmission characteristics and on the message externals, with particular emphasis on the preamble components and on routing methods; research is performed on call signs, frequencies, schedules, procedure signals, external message numbers, routing indicators, and cryptographic features, resulting in the ultimate reconstruction of the complete net with all its pertinent details.

RADIO COMMUNICATIONS

Efficient radio communications are dependent upon (1) the physical laws for the transmission, and (2) the requirements imposed by the necessities for the establishment and maintenance of communications. The first consideration involves the frequencies and power used, and the second consideration embraces the details necessary for the communications themselves, such as the call signs, routing, message numbering conventions, and receipting and servicing of the traffic. These latter items may be varied or changed by direction of the communications authority either for convenience in handling traffic, or for purposes of secrecy, or both.

From the standpoint of traffic analysis study there are three main aspects of radio operations, as follows:

The operating data. These consist of the basic operating and functioning data of the net; e. g., the structure or form of the net, the frequencies, the call signs, and the schedules.

The radio transmission. This includes the particular Morse code used, the procedure signals employed, the order of elements of the transmission, and radio operators' chatter.

The messages. These include the message texts proper, together with the message preambles and postambles. The cryptographic features of the message texts, such as discriminants and message indicators, the type of cryptographic text (whether in letters or digits), and the length of the code groups, are all of considerable assistance in traffic analysis; plain-language messages are also exploited.

OPERATING DATA

Radio stations are linked together and organized into nets for the purpose of intercommunication; this organization follows definite patterns, reflecting the command structures since the lines of communication must coincide with echelons of command in order to meet military communication requirements. In a particular grouping of stations the one serving the senior echelon is the station usually in charge of the subordinate stations; this station is called the *net control station* (abbr. NCS), and the others are called outstations. The control station is responsible for the supervision of transmissions, procedures, and circuit discipline. A typical net structure is shown in Fig. 1, below. Station 1 is the superior headquarters, with Stations 2, 3, and 4 as the immediately subordinate outstations; Station 2 in turn has two outstations, and Station 3 has three outstations. Station 1 is also in communication with Station 10, the NCS of another net.

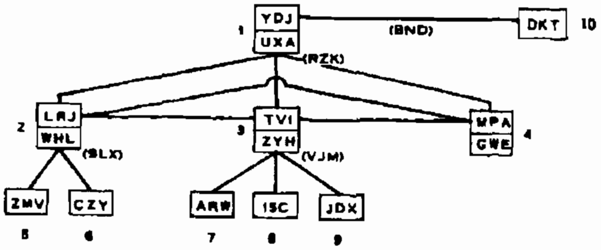


Fig. 1.

Stations are identified by one or more call signs which consist of a group of letters, digits, or both. In the diagram above, Stations 1–4 have two call signs each, while the remaining stations have but one call sign. Multiple call signs are used for convenience of operations, or for security; they are either in the form of *variant call signs* (the selection from these being left up to the radio operator) or of *split call signs* (the selection of the proper call sign being governed by the time of day, the radio frequency used, etc.).

The usual type of call-up is the double-station call procedure, wherein the call signs of the called station and of the transmitting station are sent, separated by the procedure signal DE (meaning "from"); for example, if TVI is calling UXA, he would transmit the following:

UXA UXA UXA DE TVI TVI TVI

The reply from UXA would then be:

TVI TVI TVI DE UXA UXA UXA

In the single-station call procedure, only one call sign, usually that of the called station, is used. For example, if ZYH is calling ARW, he would send ARW ARW ARW; when ARW answers, he would reply in the same manner, ARW ARW ARW.

Sometimes one particular call sign is assigned to a link, i. e., for intercommunication between two specific stations. For example, referring to Fig. 1, when Station 1 wishes to make contact with Station 10, he would send the link call sign BND repeated several times, and Station 10 would reply with the call sign BND.

In addition to the foregoing types of calls, there may also be used a collective call sign for calling several specific stations in a net; when such a call sign is used for alerting all of the stations in the net, it is called a *net call sign*. For example, Station 1 uses the net call sign RZK for reaching his three outstations, and Station 3 uses VJM as his net call sign.

In all of the foregoing procedures, split-call working might be employed As an example, we note in Fig 1 that Station 3 uses the call sign TVI when communicating with its superior, Station 1, or with Stations 2 and 4; however, when Station 3 is communicating with its own outstations, it uses the call sign ZYH.

Stations in a net are assigned one or more frequencies for radio communication; the allocation of frequencies is predicated upon transmitter characteristics, distance requirements, the time of transmission, and other factors. In *simplex* working, stations operate on a common frequency; in *complex* working, more than one frequency is used. In complex sending, stations are assigned *transmitting* frequencies, and each station uses its assigned frequencies to make contact with other stations; in complex receiving, stations are assigned *receiving* frequencies, and stations sending to a particular station use the frequency assigned to it.

The time of communication is an important factor in radio operations. Schedules for communication are established for those stations which pass comparatively little traffic, or which have an insufficient number of operators for free communication with all necessary stations; in such cases, schedules are arranged so that each operator may take care of several circuits at different times. Such schedules also permit maximum use of one frequency, without interference or confusion. When no schedules are in force, stations are free to contact each other at any time, either by setting the time for the next contact at the last transmission, or by maintaining a watch on assigned frequencies.

RADIO PROCEDURES

In radiotelegraphy the transmission of information is accomplished by means of Morse codes. In the case of countries whose alphabets differ from the English alphabet, modifications of the international Morse symbols are introduced to take care of accented and other unique letters of the language.

Radio operators use certain signals and signs to facilitate operation and passing of traffic. The most common sets of operating signals, used in international practice, are "Q" and "Z" signals, which are three-letter combinations beginning with these letters. For example, QRU means "I have nothing for you," and QRU followed by a question mark (Morse $\overline{\text{IMI}}$) means "Do you have anything for me?" Besides these operating signals, various procedure signs are used by the operators, such as the following:

$\overline{\text{AR}}$	End of transmission	GR	Group count
$\overline{\text{AS}}$	Wait	$\overline{\text{IMI}}$	Repeat or question
$\overline{\text{BT}}$	Break	K	Invitation to transmit
C	Correct	WA	Word after
DE	From	$\overline{\text{VA}}$	End of schedule

In addition to the foregoing, radio operators may be provided with a specialized cryptosystem, usually in the form of a small chart (with row- and column coordinates) containing letters, digits, words, and useful short operators' messages.

In order to prevent enemy stations from entering a net and confusing its operations, authentication systems are used. In station authentication, challenges and replies are exchanged mutually by stations upon establishing initial contact; in message authentication, certain elements from the heading and from the message text are designated by prearrangement as test elements, and these test elements are validated by an authenticator symbol or symbols in the preamble.

In military communications, a single time designation is used to avoid the confusion that would result if each station used local time as reference. Normally, Greenwich Mean Time is used for all communications, although in some instances the time zone of the capital of a country is employed; in any case, it is usual practice to include the suffix letter of the time zone, as for example 231600Z meaning 1600 Greenwich Mean Time on the 23d of the month.

There are certain elements of the transmission which are standard for most radio operations. These are: (1) the call-up, or the procedural rules by which stations make contact with one another to prepare for the transmission of traffic; (2) the order of traffic, governed by rules which determine which station is to transmit its traffic first, and in what order; (3) the transmission of traffic, in a prescribed manner; (4) the receipting for traffic, in which the receiving station acknowledges receipt of messages; (5) corrections and services, to insure that the traffic transmitted and received is as garble-free as possible; and (6) the signing off, or the procedures prescribing the manner of terminating transmissions. Variations in the number and detail of the foregoing elements exist not only among various nations, but also among the military services of a particular country and among the different echelons of these services.

RADIO MESSAGES

Radio messages must carry pertinent information to insure proper handling in both the message center and the radio station. This information, almost invariably incorporated in the message externals, usually includes serial numbers of various kinds, date-time groups, precedence symbols, routing instructions, addresses and signatures, the group count, and other special instructions.

The number which is put on the message by the transmitting radio operator for reference purposes is known as the *station serial number* (abbr. NR); a number series may be assigned to all messages transmitted by a particular station, or separate number series assigned to messages passed on each communication link. *Message-center numbers* (abbr. MNR) are numbers assigned serially by a message center to all outgoing traffic, regardless of destination; these numbers are used for reference purposes between originating and receiving message centers. When messages are relayed, the station serial numbers change on each link of the communications path, whereas the message-center number usually remains constant. Other kinds of numbers are sometimes found in message externals, especially at the higher echelons, such as cipher-office numbers or radio-station in-desk numbers.

Precedence indicators or symbols for expediting traffic are either in the form of abbreviated plain text (such as "U" for Urgent) or in encrypted form as a group of letters or digits. Sometimes variants are provided for these indicators as a security measure, or these indicators may be subjected to encipherment.

When direct communication between two stations is not possible, routing instructions are usually incorporated in the externals of messages. Designations of locations or units in plain text may be utilized for this purpose, or call signs may be used for the routing, but, more usually, routing codes are employed which contain code groups for principal locations or units, as well as syllabary groups for encoding designations not in the body of the code. Similarly, when addresses and signatures are distinct from routing instructions, a separate scheme may be devised for the transmittal of this information, usually by means of codes.

PRELIMINARY NET RECONSTRUCTION

In the initial approach to a traffic analysis problem, traffic identified by the language of plaintext chatter, or by national characteristics of the transmission, as belonging to the target country is segregated into major homogeneous types on the basis of common operating characteristics, message formats, discriminants, chatter, or any collateral information. Thus traffic from army, navy, air force, and other nets may be isolated into distinct groups.

A preliminary grouping of stations is diagrammed from observed contacts between stations. Simultaneously, analysis is begun on the characteristics of the radio operations. As an example, let us assume that the groupings of stations in Figs. 2a and b, below, have been reconstructed from observed contacts on the transmitting frequencies in kilocycles as indicated, and that we have made a mental note that, on the basis of procedural characteristics, UXA and ZYH are probably net control stations. We note that TVI and ZYH have the same frequency; if frequencies are assigned uniquely to target stations, then TVI and ZYH represent the same station. Tentative confirmation may be obtained if it is found that the serial numbers used by TVI interlock with those of ZYH, or if routing information on messages from TVI and ZYH shows identical originators; further confirmation may be obtained from chatter (wherein, for example, the operators at TVI and ZYH refer to the same person as their commanding officer), from direction-finding bearings, Morse-operator analysis, discriminant and indicator studies, etc. By continuing this method of analysis, we shall arrive at a portion of the diagram in Fig. 1, wherein TVI and ZYH are shown as split call signs belonging to one station. This example of approach is perhaps an oversimplification, but it is illustrative of the general methods followed.

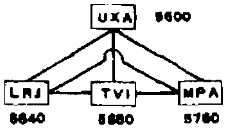


Fig. 2a.

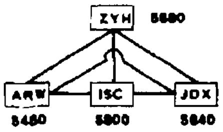


Fig. 2b.

ANALYSIS OF RADIO OPERATIONS

This phase of traffic analysis involving the study of the operating data and the elements of the transmission is, as previously stated, carried on concurrently with initial net reconstruction. When fragmentary nets have been put together, continuity over date-breaks is made possible by the analysis of radio operations.

Callsign analysis embraces the determination of the methods of generation, allocation, and rotation of call signs, together with the system of use. Call signs may merely consist of different random *n*-character groups, in which case no system of generation is recoverable, or they may be generated by a permutation table or similar scheme. The available call signs may be arranged in the form of a chart or in a book of tables, and stations may be allotted specified positions in the chart or book on, let us say, the first of the month; subsequent changes of call signs may be governed by following a prearranged route in the chart or book, or by the application of some mathematical formula. Callsign systems may also involve several sliding strips as a means of generation, with a convention prescribed for the manner of selection and rotation of the call signs derived from the strips. Regardless of the system of generation and rotation, when sufficient callsign continuity has been established, interpretation of the patterns and phenomena disclosed will permit recovery of the system.

Frequency analysis has the same general objectives as callsign analysis, *viz.*, the determination of the methods of selection, allocation, and rotation of frequencies, together with the system of use. When more than one frequency is assigned to each station, lower frequencies are generally used at night and higher frequencies during daylight, for technical reasons; certain of the frequencies may also be designated as standby frequencies. Frequency assignments may be published in chart form, with an initial allocation and rotation system similar to that used in callsign systems. Here again, continuity of frequencies will permit recovery of the system. Both in callsign and in frequency analysis, continuity may easily be obtained if some of the operating data or elements of the transmission change and some do not. Even if call signs and frequencies change daily, continuity may be established by taking into consideration any of the following: patterns of station serial numbers or message-center numbers; routing information; discriminants (especially one-time-pad discriminants which are usually unique for each link); procedural peculiarities (e. g., the use by a particular station of distinctive separator signs, tuning signals, etc.); chatter; schedules; service messages over a date-break; and direction finding and Morse operator analysis reports.

Procedure messages and chatter between operators are of particular interest in traffic analysis. When unknown procedure signals are used, or when procedure signals are encrypted, their meanings may be determined through observation and interpretation. As an elementary example, let us suppose that at 0915 an intercept operator hears TVI send to UXA on 3800 kilocycles the procedural transmission XLC 1200, after which contact with TVI is lost, and that TVI is heard calling UXI again at 1158. The inference may be made that XLC means "I shall contact you again at ___ hours," followed by the time. Or again, let us suppose that after that same transmission, contact with TVI was lost, and that the intercept operator in searching for target stations on his receiver picks up TVI a few moments later on 4800 kilocycles. In this case, it may be inferred that XLC means "I am changing my frequency to ___ kcs," followed by a frequency designator which is to be multiplied by 4 to indicate the actual frequency.

The identification of preamble components is a relatively simple matter. If messages from Station A to Station B are sorted by intercept time, the station serial numbers should be in an ascending series (barring, of course, missed traffic), so that we look for such manifestations in elements of the preamble. If all the traffic sent from one call sign, regardless of direction, is sorted by file time (where this information is included in the preamble), the message-center numbers should be in an ascending sequence, with gaps caused either by missed traffic, or because the station concerned used more than one call sign, or because some messages may have been transmitted by means other than radio. The position of originator groups in the message preamble may be discovered by sorting traffic by transmitting station and noting the consistency of certain groups in a particular position; likewise, addressee groups may be identified by sorting traffic by receiving station and looking for a high rate of occurrence of some group or groups in a particular position in the preamble. The identification and interpretation of precedence indicators may be accomplished by studying a small volume of traffic emanating from one station and comparing the file times with the intercept times; when a series of messages are transmitted by a station one after the other, the messages with higher precedence are invariably transmitted first, and study of the traffic will give clues as to the meanings of these indicators. Sometimes preambles also contain groups indicating the security classification of the messages; these groups are often difficult to identify and interpret, but nevertheless a study of chatter and of the discriminants used on the various cryptonets will permit a solution.

As may be observed from the foregoing discussion, identification and partial solution of the elements of the preamble proceed simultaneously; further study and analysis will make possible a complete solution of these elements. Additional information on radio operations can be derived through study of schedules, textual features of encrypted traffic, cryptonets, and discriminants and indicator usage. Collateral information will be of assistance in these studies, as will information derived from cryptanalysis and other communication intelligence sources.

TRAFFIC INTELLIGENCE

The last phase of traffic analysis is the reconstruction of the complete enemy network in the form of an integrated diagram showing call signs, frequencies, and other technical data such as serial-number allocations, discriminants, etc. Identifications of unit organizations and their geographical locations are shown, which, when coupled with intelligence from all sources, will portray the enemy Order of Battle.

When changes in net structure take place, these may be brought about by the appearance of new units in a command or the deactivation or redeployment of old units. Changes in contact relationship may be indicative of impending moves; significant changes in traffic volumes or in cryptographic systems may be indicative of preparations for military activity.

CONCLUDING REMARKS

Traffic analysis furnishes much information on communications features of assistance in cryptanalysis, such as information concerning the originators and addressees of the messages, isologs and resends which result from cryptographic error, messages with potential crib value, and chatter pertaining to cryptographic matters.

Some traffic analysis items of particular interest to the cryptanalyst are the following:

When the group count is constantly checked by the enemy operators, this is usually indicative that the cryptosystem includes transposition as one of its steps.

When the date or file time is invariably checked, it is indicative that these elements are factors in key selection.

When a group in a particular position of the text or of the preamble is checked frequently, this may indicate that it is involved in key selection.

Rapid sending, with no requests for services by the receiving operator, is an earmark of practice or dummy traffic.

The general principles of traffic analysis have been presented briefly in the preceding paragraphs; however, as with cryptanalysis, a real understanding of these principles and techniques can come only with practical application.

Science and Cryptology

BY HOWARD T. ENGSTROM

~~Secret~~

The address at the first meeting of the NSA Crypto-Mathematics Institute.

Ladies and Gentlemen: I hope that my address to you this morning, if it can be called an address, will not be considered as an example of your future proceedings. I am unprepared. Now that I have become a manager, I have given up such childish things as working, particularly in the technical area. I might say it is with considerable regret that I have given up these very fascinating things. The establishment of the Crypto-Mathematics Institute is a great step forward in the progress of the National Security Agency. The address that I shall attempt to give you this morning will not be marked by examples of scholarship and accuracy. In fact, any remarks I make are subject to future revision, since I have not had the time to verify certain dates and facts.

I've chosen as my subject "Science and Cryptology." Of course, a natural way to begin a discussion of this sort is to attempt to define the terms. I have spent a little time during the last few days looking for a good definition of science but, unfortunately, I haven't been able to find one. It is a rather complex concept. It has something to do with observation versus authority. It has something to do with knowledge of natural laws versus superstition. Mr. Bertrand Russell states that modern science is about three hundred years old. I think we all understand approximately what science is and the impossibility of giving a definition of it in a few sentences. On the other hand, one might ask what is cryptology? Cryptology really is older than science in the modern definition. Certainly it existed at the time of Caesar and before. It has essentially two parts to it, as you all know; one is the concealment of your meaning from a possible enemy and the other is unraveling the meaning concealed in such a message or such a writing. I believe that the impact of science on cryptology probably started in this century. I suppose one can blame a great deal of our troubles on Marconi, or go further back to Hertz and perhaps even to Maxwell and Faraday, who discovered the natural laws that enable us to convey meaning through electromagnetic phenomena. Marconi and the radio came in in the early 1900s, perhaps 1910-1914. They made the problem of the cryptologist somewhat more complicated, in that he no longer had a piece of paper delivered to him which contained some meaning, but had to plumb the depths of the atmosphere to extract his raw material. Many other things which had an impact on cryptology and might be called scientific, happened in this century. For example, in the early twenties, one of the achievements was the invention of the flip-flop circuit. Two men, Jordan and Eccles, in 1919 got out a patent on a circuit involving two vacuum tubes. This circuit had the remarkable property of having two states which could be changed just as you turn off and on an electric light, and this could be done in a matter of microseconds. Here is an example of fairly pure science. What use can be made of such a device triggered by electronic pulses at microsecond rates? Electronic counters making use of the Jordan-Eccles flip-flop circuits were developed to considerable perfection in the thirties and used in the study of cosmic ray phenomena.

Things happened in the field of cryptology during this period of which perhaps the most significant was the introduction of the wired wheel, which you are all familiar with. In the early twenties, an old gentleman named Hebern from California came to the Navy Department with some drawings on a piece of wrapping paper indicating the original form of a wired-rotor device for use in encipherment. During the twenties and the thirties, the use of wired-wheel machines extended considerably and in World War II, of course, they were a principal means of encipherment. Now, through the introduction of wired wheels in cryptography, the necessity for the use of advanced techniques in solving some of these devices became evident. When I came into the Navy in 1941, I was presented with problems involving the solution of a German cipher machine which was based upon the wired-wheel concept. This required the application of very high-speed techniques. During World War II, we built approximately 150 large-scale electronic devices, including electronic counters, to solve the cryptanalytic problems imposed upon us by the use of wired-wheel machines. I might say that our successes were considerable. The tantalizing thing about the situation in 1941 and 1942, particularly in the Battle of the Atlantic, was that although we knew how to solve the problem, principally from researches carried out by the British, a tremendous amount of equipment was required. It took us two years to get this equipment into operation, and during this period, of course, the number of sinkings in the Atlantic was enormous. We were struggling to create something in the development sense and in the production sense, that would solve problems which we knew very well how to do. On the cryptanalytic side, the problems in World War II were extremely challenging, and we developed a number of original cryptanalytic methods based upon the capability of performing operations at these very high speeds. We explored many methods of handling these problems. [redacted] Many physical scientific ways of doing the job were explored. We had a great deal of work at the Eastman Kodak Company in which recording was done with spots on film, and scanning by optical means; we did the digital work principally at the National Cash Register Company; we put forth every effort to explore all possible means of solving these cipher problems.

It was not only in this area that science had an impact on our successes in World War II; we also became increasingly conscious of the problems of propagation. In 1942, the British sent over a delegation who were quite disturbed at our lack of knowledge of the upper atmosphere, the "E" layers and the "F" layers and the phenomenon of ionic reflection. Admiral Redman, who was then Chief of Naval Communications, commissioned me to form some sort of organization to explore these phenomena. I managed to get started an organization called the Inter-Service Ionospheric Laboratory, which has since become the Central Propagation Laboratory at the Bureau of Standards, where phenomena of propagation through the upper atmosphere are studied. Sounding stations in many places were established in order to determine the heights of various layers, the maximum usable frequencies, the optimum assignments of our intercept positions—the problems became quite intricate. We studied such problems as identification, [redacted] problems of direction-finding, which are still with us, and location of transmitters through various means of detecting phase differences,—times of arrival. In other words, the problem of cryptology in World War II involved not merely a matter of reading some ciphers on a printed page, but had become an extremely scientific matter of extracting information from the atmosphere around us by the use of all possible scientific means available. At the end of World War II, everyone appreciated the necessity for the application of modern science to NSA problems.

In the late forties, NSA established the Scientific Advisory Board. The best scientists in the country have been called to see if they could help us and suggest ways of analyzing some of our complex problems. We were extremely fortunate, for example, in having a person like John von Neumann, who was considered one of the outstanding mathematicians of his time, as a member of our Scientific Advisory Board, and I could mention many more names of outstanding individuals in Science who have examined our problems. We have ourselves been searching for new scientific methods of attack. A project was started at the University of California at Los Angeles, in an organization

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

called SCAMP, in which for three months each summer a group of outstanding mathematicians get together to consider our problems in the broad sense. [redacted] The mathematical advisory panel of the Scientific Advisory Board has examined our work. They have said that, to their knowledge, there exists no discipline in mathematics having a potential application to our problems that has not been explored, and explored in an extremely efficient way.

[redacted]

We have tried to apply many disciplines of mathematics to our field. It seems fairly elementary that the science of group theory should be applicable in our business, which is concerned a great deal with permutations, which certainly form a group, but the efforts to apply group theory to our problems have not been particularly fruitful. Group theory does not seem to contain the key to the things that we want to do.

Another thing that has happened to us in the period since 1946 is the tremendous development of the communications art; the problems of searching for and extracting from the ether the things that we are interested in are becoming extremely difficult. We are faced with problems of speech encipherment, facsimile encipherment, television privacy, IFF, and data links for the control of aircraft. These many new forms of communication mean that it is essential to maintain a very forward scientific posture. We have tried to see whether there are any implications of the Information Theory as developed by Nyquist and Shannon which will assist us in our attempts to find meaning in these various transmissions. The problems of communications intelligence and those of what we call electronic intelligence, or ELINT, are becoming more and more merged. The distinction between what communications and what control signals are grows increasingly fuzzy.

With these remarks, I hope that I have succeeded in establishing some relationship between the progress of science and the problems of cryptology, both in the cryptographic and the cryptanalytic sense. NSA can be rightly proud of its position in stimulating research toward its mission. We had a considerable part to play in the development of the modern internally controlled calculators, the large-scale digital computers. I think the first large-scale digital computer in operation was the 1101, which was essentially designed by NSA people. They played a tremendous role in the development of these large-scale computing devices. Now also in the last years we can be justly proud that we have stimulated people like [redacted] who have pioneered in the low temperature cryotron in connection with digital computers. We pioneered through one of our people, [redacted] the work in deposition of films by evaporation for use in the magnetic memories. NSA has played a central role in many of these basic researches in computation. Now, the question always arises in connection with budgets and money: is it necessary for NSA to sponsor this basic research? Why can't institutes like the National Science Foundation, the Office of Naval Research, and so on, take care of this fundamental progress in science which is necessary to us? Why do we have to spend our money for this sort of thing? In fact, when I first arrived here, I got into trouble with the Bureau of the Budget because R/D had been spending some of its money in support of solid propellants for rockets, and this seemed to be a bit far-fetched. The reasons for it were principally good, and our interest in the upper atmosphere was such that we wanted to get some instruments up there to see how things are. However, I couldn't establish the justification for NSA's supporting work in solid propellants—we must stick more closely to our own last.

Now we are definitely supporting certain things in the way of basic research. The needs of NSA in high-speed computing are unique. As a result, we have established a project called LIGHTNING in which we are exploring the possibilities of computation [redacted] I might say that we are doing this in a rather free-hand manner at the moment. We have three major companies engaged in the field: RCA, IBM, and Sperry-Rand, who are going their independent ways. We feel that we should let them go for a year or eighteen months and then see if we can figure out which is the most promising approach and try to head the work in that direction. The Laboratory for Electronics at M. I. T., under Professor Wieaner, is participating to a smaller extent in this program, as is Philco with its work in connection with special transistor devices. The work in

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

connection with the LIGHTNING project [redacted] [redacted] A year ago, we were highly skeptical as to whether speeds of this order of magnitude could be achieved. Now, I should say, it looks quite possible that at the end of the five-year program we shall indeed be able to construct computers that operate with this speed. We are now doing another thing to promote the application of science to cryptology. We have recently had a committee looking over our work, reporting to President Eisenhower, under [redacted] of the Bell Laboratories. The first recommendation that [redacted] made in his report was that there be established an Institute outside of NSA devoted to basic research problems; an Institute with an academic atmosphere which would not be subject to the tremendous pressures to which you all are subject—pressures to solve immediate problems as against thinking about the long-range future of the art. A report has been submitted to the President, who said by all means to set up such an Institute. We are now in the process of doing so. I can't tell you where it will be, but we shall establish something of a basic research nature. I hope in the next few months to be able to report that this has been achieved.

(b)(3)-P.L. 86-36

I trust that I have been able to convey to some small degree the impact of science on cryptology. There are people—and very distinguished people—who still feel that cryptology is an art. I think it is an art, but I don't see how the results in the modern type of security of communications and electronic dissemination can be achieved without drawing upon the tremendous accomplishments of modern physical and mathematical science.

I might say in closing that I came back from industry partly with the idea that perhaps I could contribute something to the Agency, but I think the principal reason was that I have never worked with such a stimulating group of people as I find in NSA.

A New Concept in Computing

BY [redacted]

(b)(3)-P.L. 86-36

Unclassified

A new computing scheme was proposed by von Neumann in a patent[1] *submitted in 1954 and granted posthumously last December. This paper is an explanatory statement of the ideas embodied in the patent, with other related topics.*

INTRODUCTION

Von Neumann recognized the limitations of computing speeds inherent in the existing technology due to device operation times, signal propagation delays, and transmission distortion of information video pulses. Of course we cannot reconstruct the thinking that led him to the proposed solution, but the attractiveness of large bandwidths which could be obtained at microwave frequencies and of representation of digital information by distinct phases of an RF signal (neither of which had been exploited in computer technology) no doubt seemed fertile ground for investigation. Whatever the prompting force was, von Neumann proposed a computing scheme using RF techniques which is potentially faster if employed at microwave frequencies than present conventional methods. The same methods will also work at lower frequencies.

The availability of an element of the following nature was assumed:

a. An element is available that has both L and C, one of which is nonlinear.

b. The dissipation in the element is not great in comparison to the nonlinearity. This dissipation may be resistive loss or a hysteresis.

c. The element has approximately linear operation for small signals and has a resonant frequency (which is later referred to as f_0).

NONLINEAR REACTANCE ANALYSIS

To see that such an element can exist, consider the nonlinear capacitor that has no loss and no hysteresis[2], and is mounted in multiply-tuned circuits. The bare outline of the analysis will be presented.

[1] "Non-linear Capacitance or Inductance Switching, Amplifying, and Memory Organs", John von Neumann, U. S. Patent No. 2,815,488, issued 8 December 1957.

[2] These restrictions may be relaxed somewhat in the practical case, but are assumed here to make explanation simpler.

(b)(3)-P.L. 86-36 [redacted]

Full discussion of it has been published by Manley and Rowe[4]. As pointed out in that reference, consideration of nonlinear reactances as elements to transfer power from one frequency to another is not a new subject, having been discussed by Hartley in 1916.

Consider the circuit in Fig. 1.

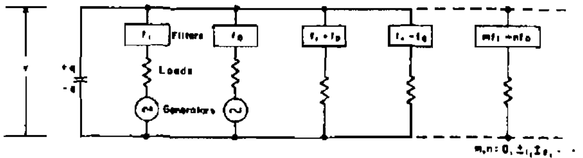


Fig. 1.

$v = f(q)$ is an arbitrary, single-valued function, being in general nonlinear.

The filters have zero impedance at the labeled frequency and infinite impedance otherwise.

Such a circuit might be a number of tuned circuits in parallel with the nonlinear reactance (which also may be inductance rather than capacitance). Two of the tuned circuits contain RF generators.

The charge on the capacitor, the current into it, and the voltage across it may all be expressed as double Fourier series in the frequencies $mf_1 + nf_0$ for $m, = 0, \pm 1, \pm 2, \cdots$. By manipulation of these expressions[5] one may derive others giving the summation of real power at all frequencies into the nonlinear element in terms of double integrals over complete cycles of f_1 and f_0 wherein the integrand is $v = f(q)$.

The variable q, hence $f(q)$, is periodic in f_1 and f_0 and thus for an element without hysteresis these double integrals are identically zero. From this are obtained the Manley-Rowe conditions, namely:

$$\sum_{m=0}^{\infty} \sum_{n=-\infty}^{\infty} \frac{mW_{m,n}}{mf_1 + nf_0} = 0 \qquad m, n = \text{integers}$$

$$\sum_{m=-\infty}^{\infty} \sum_{n=0}^{\infty} \frac{nW_{m,n}}{mf_1 + nf_0} = 0,$$

where $W_{m,n}$ is the real power at frequency $mf_1 + nf_0$ *into* the nonlinear reactance.

Of course, a reactance without hysteresis, whether linear or nonlinear, can dissipate no energy. Therefore, as must be true and as can be obtained from the above conditions, the summation of energy at all frequencies into the reactance is zero, and power supplied from one source at a given frequency will show up in another branch of the circuit at another frequency. The exact manner in which this takes place is controlled by the above conditions.

The circuit initially pictured was a general circuit; variations of it may lead to modulators, demodulators, amplifiers, oscillators, or combinations of them. Of interest to this discussion is a sub-harmonic generator as shown in the circuit of Fig. 2.

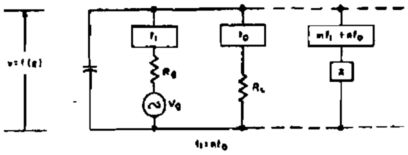


Fig. 2.

V_G is an RF generator, essentially an AC power supply. The f_1 filter and R_G correspond to the resonant tank of the RF generator. The f_0 filter and R_L are the load tank at the sub-harmonic frequency desired. The filters at all other frequencies are terminated in pure reactances, X, which for simplicity may be open or short circuits. There will be no power loss at these other frequencies.

The only terms of interest in the Manley-Rowe conditions are for $(m, n) = (0, 1)$ and $(0, n)$. The rest of the $W_{m,n}$ are zero. This gives:

$$\frac{W_{0,1}}{f_0} + \frac{nW_{0,n}}{nf_0} = 0,$$

or simply

$$W_{0,1} = -W_{0,n}.$$

The minus sign indicates that all the energy put into the nonlinear reactance at the $f_1 = nf_0$ frequency is transferred to the load tuned to the f_0 frequency. This is a harmonic generator with an ideal efficiency of 100%, assuming no losses in the reactive termination of the other frequencies. Of course with real elements some losses, and resultant reduction of efficiency, will occur, but the basic (sub-)harmonic generation process, unlike that of Class C multipliers or crystal multipliers, is not limited in efficiency.

[4] "Some General Properties of Nonlinear Elements—Part I. General Energy Relations", J. M. Manley and R. E. Rowe, *Proc. of IRE*, Vol. 44, No. 7, pp. 904–918, July 1956.

[5] Complete discussion is given in reference 8.

NATURE OF NONLINEARITY REQUIRED

It remains to show that an element with a threshold of sub-harmonic generation is possible. The transfer function for such an element is shown in Fig. 3.

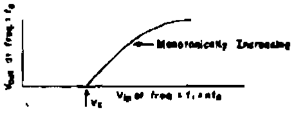


Fig. 3.

The reactance function shown in Fig. 4 is, of course, idealized. In the actual case only a smoothly varying reactance would be obtainable which could be approximated by the straight lines of Fig. 4. At V_m the nonlinearity produces a negative resistance great enough to overcome passive circuit losses. At this level of the RF power supply, the circuit would break into oscillation at the sub-harmonic frequency and the threshold action is obtained. For $V_{in} > V_t$, the amount of signal $V_{in} - V_t$ will be effective in producing sub-harmonic voltage.

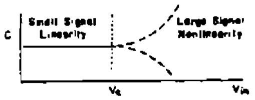


Fig. 4.

DEVICES

Various solid-state elements have been proposed to perform the function of the nonlinear reactance.[3] An equivalent circuit for a nonlinear capacitance, as realized with a semiconductor diode, is shown in Fig. 5.

(b)(3)-P.L. 86-36

[redacted]

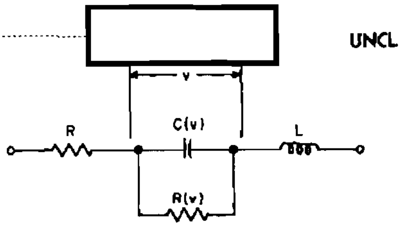


Fig. 5.

v = Barrier voltage
R = Bulk resistance
$R(v)$ = Barrier resistance (which may be nonlinear)
L = Lead inductance
$C(v)$ = Barrier capacity (nonlinear)

The barrier capacity is the primary nonlinearity of the device. Among these components the following relationships are assumed:

(1) $R(v) \gg R$ } (The element has a reasonable Q.)
(2) $R_0 = \sqrt{L/C_s} \gg R$, C_s = small signal $C(v)$ }
(3) $f_0 = 1/(2\pi\sqrt{LC_s})$ { (Tuned to the sub-harmonic frequency desired.)

This equivalent circuit as drawn includes both linear and nonlinear reactances. These may be physically separated in real devices. Research is being done on other practical means of achieving sub-harmonic response.

INFORMATION IN TERMS OF PHASE

The phase of the f_0 signal is determined by the phase of the f_1 signal. Qualitatively, this may be understood by observing, that the oscillations in the f_0 circuit are not like the oscillations in an ordinary negative resistance oscillator, in which the power supply is d-c and the phase of the oscillation is determined by noise when the oscillator is turned on. The nonlinear-reactance sub-harmonic generator is more akin to a crystal harmonic generator in which power is transferred from one frequency to another by a nonlinear element. This is true even though the action of the nonlinear reactance device in general may be explained in terms of the apparent negative resistance reflected into each appropriate branch of the circuit.

Eliminating any constant phase shift between the fundamental and the nth harmonic, th: phase relationships are examined more closely in Fig. 6.

In the example in which $n = 3$, the two signals are assumed in phase at $t = 0$. (The $n = 3$ example is chosen deliberately to point out im-

[3] "Two-Terminal P-N Junction Devices for Frequency Conversion and Computation", by Arthur Uhlir, Jr., *Proc of IRE*, Vol. 44, No. 9, pp. 1188–1191, Sept. 1956.
"The Theory of the Ferromagnetic Microwave Amplifier", H. Suhl, *Journal of Applied Physics*, pp. 1225–1236, Nov. 1957.
"Semiconductor Capacitance Amplifier", Frederick Dill, Jr. and Louis Depian, *IRE Convention Record*, Part 3, pp. 172–174, 1956.
"Small-Signal Measurements on Planar P-N Junction Diodes". A. E. Bakanowski, *Task 8 Report on Crystal Rectifiers*, Bell Telephone Laboratories, 15 April 1955.
"Frequency Conversion in P-N Junction Devices", A. Uhlir, *Task 8 Report on Crystal Rectifiers*, Bell Telephone Laboratories, 15 January 1955.

(b)(3)-P.L. 86-36

[redacted]

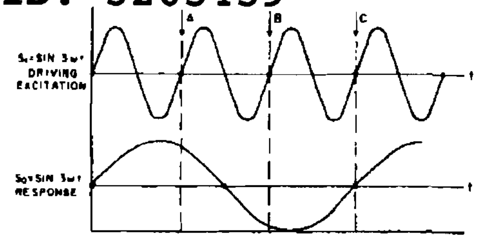


FIG. 6.

portant relationships and to avoid the $n = 2$ case, in which simplicity may cause some essential points to be overlooked.) One full cycle of S_1 later, at point A, S_1 is the same as it was at $t = 0$, but S_0 has a relative phase shift of $2\pi/3$. Similarly, at point B, S_1 is the same again, but S_0 now has a phase shift of $4\pi/3$. At point C, S_0 has a phase shift of $6\pi/3 = 2\pi$ or, like S_1, the same relative phase as when $t = 0$. Thus there are, for $n = 3$, three indeterminate phase relationships between S_0 and S_1, because in the continuous wave, S_1, one cycle is just like another. In the general case there are n such indeterminate *relationships between the RF power supply (S_1) and the induced sub*harmonic response (S_0), each of which can represent a logical state.

PHASE SELECTION AND CONTROL

If the power supply (S_1) is increased from zero amplitude past the critical amplitude, V_c, a sub-harmonic response S_0 will appear when the amplitude of S_1 is V_c. Since which of the n possible phases of S_0 will result is indeterminate, noise, or—indifferently—a small S_0 signal from another element, will dictate which phase will appear. Once the harmonic response has started, however, no external signal of less magnitude than $|S_0|$ can change the phase of the response. A simple cycle can be diagrammed (Fig. 7), plotting envelope amplitudes only. The S'_0 signal would have no effect if present at any other time than when $|S_1| = V_c$ and is increasing. Note that:

$\lvert S_0\rvert > S'_0$		(Amplification)
Duration of S_0 > Duration of S'_0		(Memory)
Phase of S_0 = Phase of S'_0		(Control or Toggle Action)

For practical realization of any computing scheme the electrical process must have natural or built-in margins. Noise, stray-signal pickup, slight misadjustment of circuits, component changes with age, all can cause a certain malfunctioning of the equipment, if the parameters which determine the action of the machine must have precise values to cause action. For, in practice, action must occur if the appropriate parameter falls within a certain region, or margin, about the ideal value.

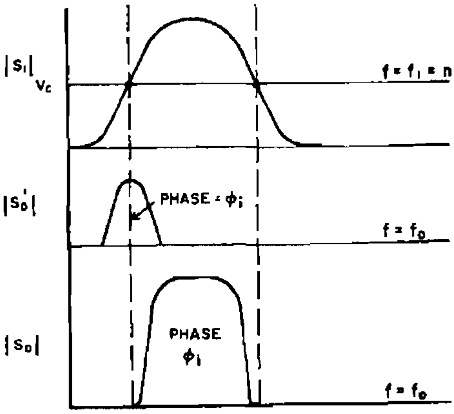


FIG. 7.

The controlling signal, S'_0, has up to now been assumed to coincide exactly with one of the n possible phases, Φ_i, of the response, S_0, and to cause S_0 to respond with that phase, Φ_i.

In Fig. 8, the phase of S'_0 is shown as being closer to the phase Φ_0 than either Φ_1 or Φ_2. The system will stabilize with S_0 at phase Φ_0, since this requires the minimum amount of energy in the presence of the S'_0 signal to respond at the Φ_0 phase as compared with the other possible phases. The figure is not intended to illustrate the exact duration (in terms of number of cycles) of the transient condition, but is only a qualitative picture. The duration of the transient will depend on the rate of build-up of the S_1 envelope and the ratio of the response S_0 to the control S'_0 during and after the start of the response. The magnitude of $\Delta\Phi$ and the effective damping constant of the transient condition will also be important.

One may conclude from this that the phase-locking property of the sub-harmonic generator has natural margins, and hence is a practical method.

AGGREGATES OF ELEMENTS

In order to control the flow of information in a logical machine, ways

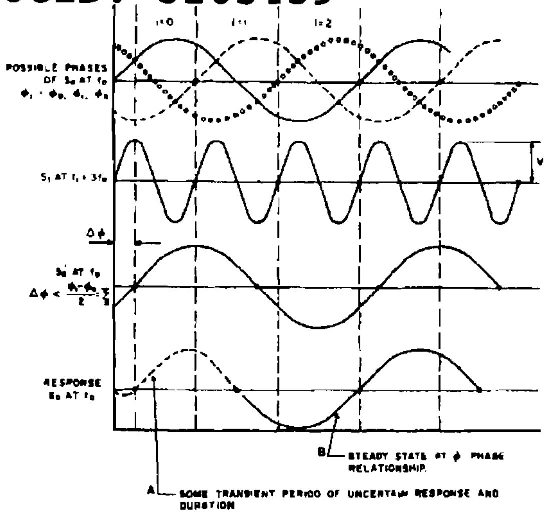


Fig. 8.

must be devised to establish an order of control. For example, if information is to flow from *A* to *B*, then *A* must control *B* but *B* must not control *A*. Ordinarily this is no problem, because the non-reciprocal devices normally used in a logical circuit to provide gain or gating perform this function automatically, but in this case one must consider the control problem separately.

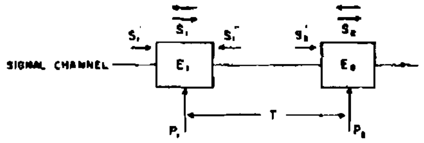


Fig. 9.

It is now necessary to devise a diagrammatic model of devices and their interconnection (see Fig. 9). The following symbolism and nomenclature will be used:

E_1, E_2 are elements such as have been described.
P_1, P_2 are amplitude-modulated AC power supplies.
S_1, S_2 are the output signals of E_1, E_2, respectively.
S'_1, S'_2 are the controlling signals for E_1, E_2, respectively.
S''_1 is the signal reaching E_1 from E_2.

The signal channel is an electromagnetic propagation path which permits propagation in either direction. The response S_1, from E_1, travels in both directions on the signal channel. The problem is to make E_1

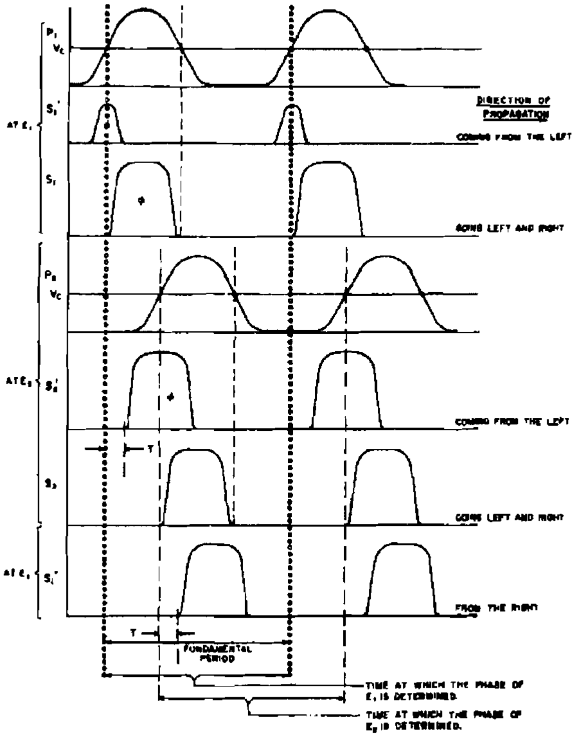


Fig. 10.

(b)(3)-P.L. 86-36 [redacted]

control E_2 and not the reverse. Let T be the time delay of the signal between elements E_1 and E_2. Consider next the timing sequence in Fig. 10.

With the timing cycle as pictured, E_1 can control E_2 but E_2 cannot control E_1. If the relative timing (i. e., the order of occurrence) of the P_1 and P_2 modulation is reversed, the direction of control is reversed.

To prevent signals other than those from next neighbors from forcing synchronization with the wrong phase, an attenuator is placed in the signal path between each element. Stray signals will have had to pass through at least two attenuators, instead of only one, so that unwanted signals will not have a major influence in determining the phase of the sub-harmonic response. The natural margins of the process enable this to work properly.

With the simple combination of elements described above, not much can be done. If, however, three classes of elements are used as shown in Fig. 11, and the timing principles discussed above are employed, all logical operations can be realized. Classes of elements are defined by the timing of the modulation of the AC power supply, as shown in the figure.

The elements of classes A, B, and C are shown interconnected by signal paths. Their respective power supplies have modulation as illustrated. The delay between elements is assumed to be negligible with respect to the power-supply modulation period. *Recalling that the phase of the response is determined by the phase of signals from other elements present when the power supply passes the critical level (the heavy dots in the diagram), observe at each dot which other element is ON.* For example, at (1) in the diagram P_a is passing the critical level, element B is off, and element C is on. Therefore, C controls A. Similarly, at (2), A controls B, and at (3), B controls C. Putting a delay between elements equal to one third of the period of the power-supply modulation, as in Fig. 12, inverts the order of control. The exact fraction of a cycle needed to do this is related to the number of different types of elements (i. e., A, B, C, . . .). Three is the minimum number of types required, and results in the simplest hierarchy of control.

This order of control is independent of which phase is induced in the controlled element by the controlling element. Similarly the number of classes of elements is independent of the number of possible phase states.

The delays referred to above are in terms of *group velocity* with respect to the power-supply modulation period. This period has been assumed to be long compared to the period of the sinusoidal signals involved, so that adjustments of delay to fractional cycles of the sinusoidal voltage in the signal channel will not affect appreciably the delays previously discussed. Consider now the *phase velocity* of the signal channel. The phase induced in the controlled element will depend on the phase delay between it and its controlling element. A phase Φ_i in the controlling element *after* a phase delay K would put the controlled element into phase state $\Phi_i + K$. For the binary case, the phase shift K would be either an even or an odd multiple of π.

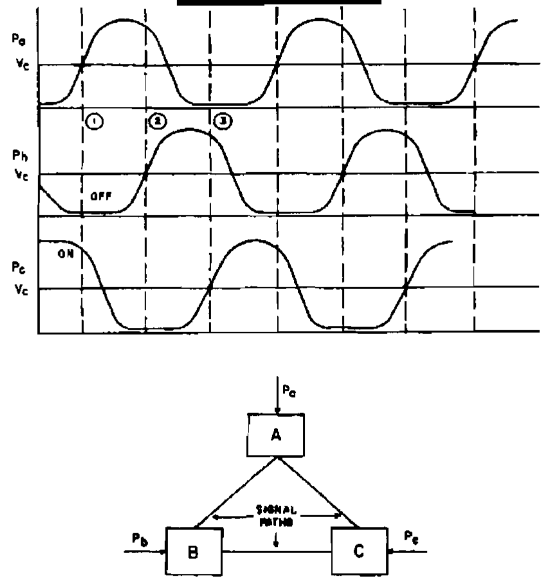


Fig. 11.

Up to this point all discussion has admitted the possibility of n phase states, or equivalently that $f_1 = nf_0$, where n is any integer. The elements can thus be used to implement n-state logic. At this point complete generality will be dropped, and we shall proceed to illustrate how these principles can be applied to build up binary logic with $n = 2$. With minor changes in the illustrations an n-state logic can also be realized.

Collecting nomenclature and graphical conventions which have been used, a lexicon of terminology for $n = 2$ is shown in Fig. 13.

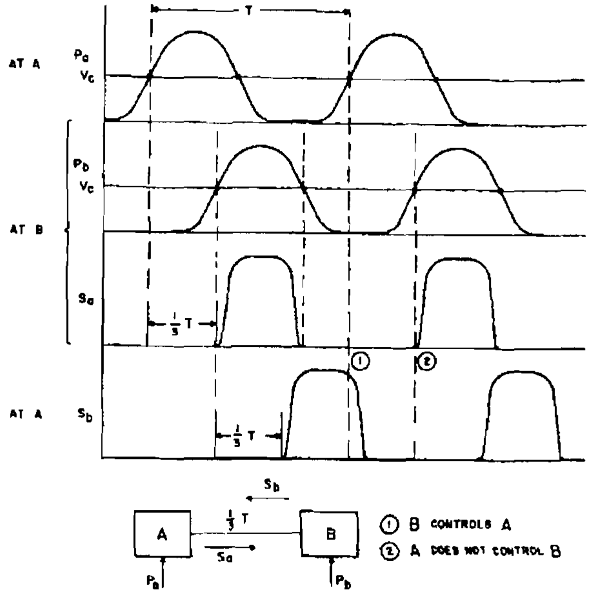


Fig. 12.

MAJORITY LOGIC

The chief value of the aggregates of sub-harmonic generators is that they can be used to perform majority logic. By definition, a majority organ is a device or circuit which has multiple inputs and a single output. The value of the output is the value of the majority of the inputs. To avoid the indeterminate case, there must be an odd number of inputs.

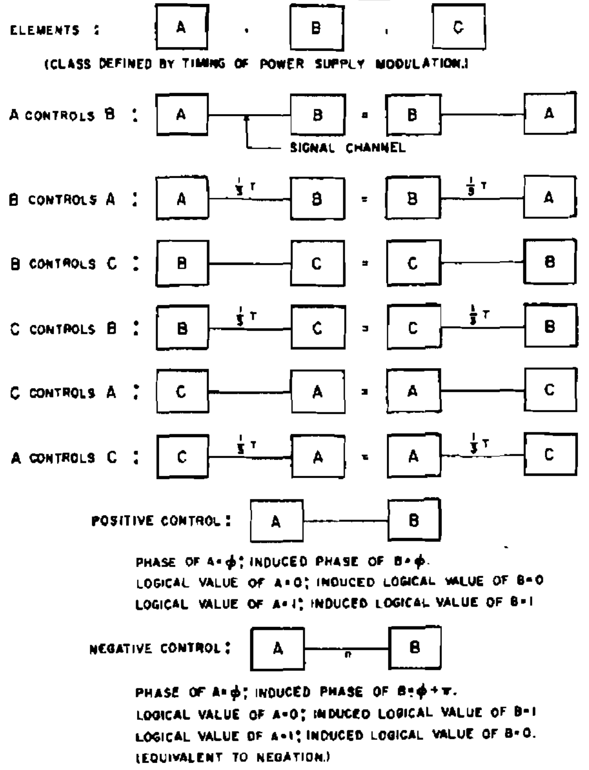
In Fig. 14 the linear addition of signals from three A elements is applied to a B element.

$$\begin{aligned} \text{Let } S_{a1} &= E\cos(\omega_0 t + \Phi_1) \\ S_{a2} &= E\cos(\omega_0 t + \Phi_2) \\ S_{a3} &= E\cos(\omega_0 t + \Phi_3) \end{aligned}$$

where $\Phi_1, \Phi_2, \Phi_3 = 0, \pi$, depending on the state of each A element, and $\omega_0 = 2\pi f_0$, the angular frequency of the sub-harmonic response. Possible results for S_a are:

(b)(3)-P.L. 86-36

[redacted]



PHASE OF A=φ; INDUCED PHASE OF B=φ.
LOGICAL VALUE OF A=0; INDUCED LOGICAL VALUE OF B=0
LOGICAL VALUE OF A=1; INDUCED LOGICAL VALUE OF B=1

PHASE OF A=φ; INDUCED PHASE OF B=φ+π.
LOGICAL VALUE OF A=0; INDUCED LOGICAL VALUE OF B=1
LOGICAL VALUE OF A=1; INDUCED LOGICAL VALUE OF B=0.
(EQUIVALENT TO NEGATION.)

Fig. 13.

$$\begin{array}{rl} E\cos(\omega_0 t + 0) & \text{two } \Phi_i = 0, \text{ one } \Phi_i = \pi \\ E\cos(\omega_0 t + \pi) & \text{two } \Phi_i = \pi, \text{ one } \Phi_i = 0 \\ 3E\cos(\omega_0 t + 0) & \Phi_1 = \Phi_2 = \Phi_3 = 0 \\ 3E\cos(\omega_0 t + \pi) & \Phi_1 = \Phi_2 = \Phi_3 = \pi. \end{array}$$

Since the information is carried in the phase, S'_a has either 0 or π phase depending on the majority of the phases of S_{a1}, S_{a2}, and S_{a3}, and since the phase of S_b is determined by the phase of S'_a, then

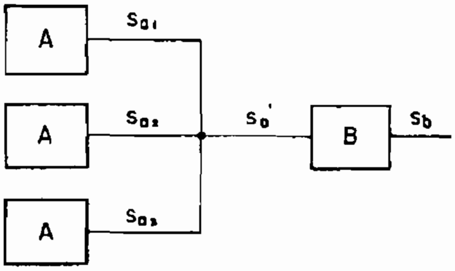


Fig. 14.

$B = \text{Maj}(A_1, A_2, A_3)$. The amplitude variation has no importance. The truth table and equivalent logical expression are as follows, arbitrarily letting $\Phi = 0$ be state "0" and $\Phi = \pi$ be state "1".

A_1	A_2	A_3	B
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

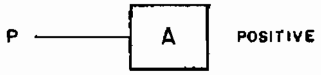
$B = A_1 \cdot A_2 \cdot A_3 + (A_1 \cdot A_3 + A_1 \cdot A_2 + A_1 \cdot A_3)$

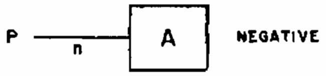
WHERE "·" IS INTERSECTION,

AND "+" IS CONJUCTION

The majority organ and a negation operation (as shown in Fig. 13) are sufficient to build all logic.

The only thing lacking at this point is a method for putting information into such a system. Permanent sources at the f_s frequency which are gated on when desired by external controls, fill this need. A permanent source can control any class (A, B, C) of element. There are two possible types of permanent sources:



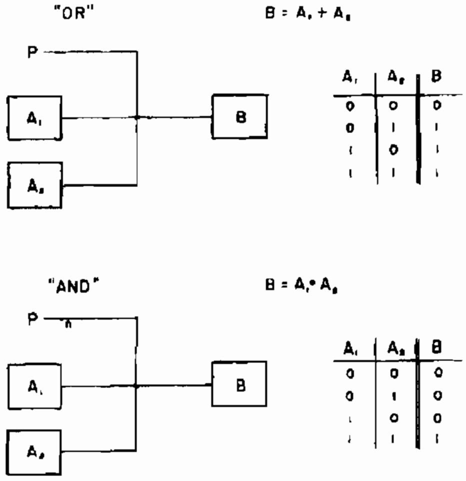


The reference permanent source p is assumed to have state "1".

(b)(3)-P.L. 86-36

[redacted]

By using majority organs, negation, and permanent sources, the elementary logical operations shown in Fig. 15 can be performed. (At this point the separate designation of S_a as being a response of an element, A, will be dropped. The logical state represented by S_a will be called simply the *state or binary value* of A.)



A_1	A_2	B
0	0	0
0	1	1
1	0	1
1	1	1

A_1	A_2	B
0	0	0
0	1	0
1	0	0
1	1	1

Fig. 15.

The use of the majority organ also allows realization of other nonelementary logical functions. One of its great values is that a single organ can be used to realize many logical operations by what might be called logical biasing. This is shown in Fig. 16.

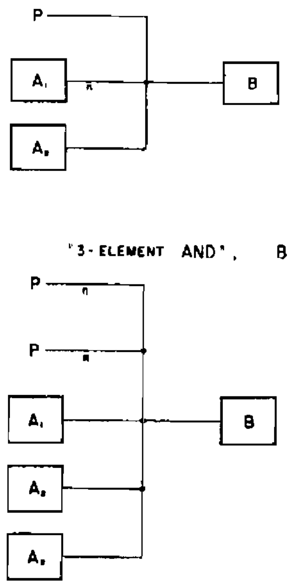
The above may be generalized in an obvious way to n elements. Also, an n-element "or" circuit differs from the "and" circuit only in having a positive rather than a negative relationship for the permanent sources. One other important aggregate is the "parity" circuit (Fig. 17).

$B_1 = \text{Maj}(A_1, A_2, A_3)$ $\qquad C = B'_1 \cdot B'_2$
$B_2 = A'_1 \cdot A'_2 \cdot A'_3$ $\qquad A_4 = B_3 + C$
$B_3 = A_1 \cdot A_2 \cdot A_3$

$$\therefore A_4 = A_1 \cdot A_2 \cdot A_3 + \{[\text{Maj}\ (A_1, A_2, A_3)]' \cdot (A'_1 \cdot A'_2 \cdot A'_3)'\}$$
$$= A_1 \cdot A_2 \cdot A_3 + [(A_1 \cdot A_2 \cdot A_3) \cdot (A'_1 \cdot A'_2 \cdot A'_3) + (A_1 \cdot A_2) + (A_2 \cdot A_3) + (A_1 \cdot A_3)]'$$

"IMPLICATION" $B = A_1' + A_2$

"3-ELEMENT AND", $B = A_1 \cdot A_2 \cdot A_3$



A_1	A_2	B
0	0	1
0	1	1
1	0	0
1	1	1

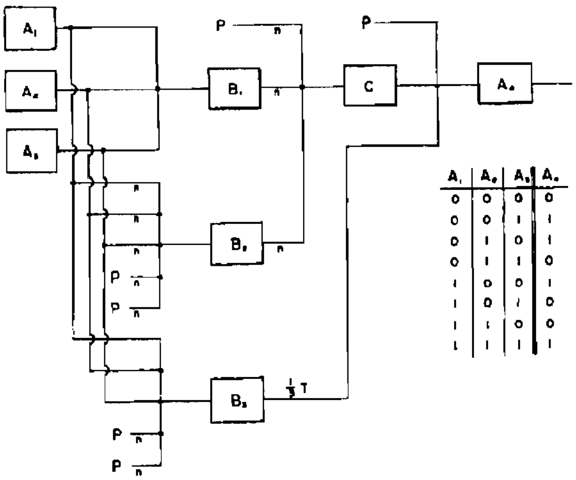
A_1	A_2	A_3	B
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

Fig. 16.

As an example of the performance of a specific non-elementary logical operation, we show the majority organ and the parity circuit combined to make one stage of an adder (Fig. 18).

Reviewing what has been discussed: after establishing that the phase of the sub-harmonic response of a "tuned" nonlinear reactance can be used to represent logical states, the processes of negation and majority were shown to arise naturally. From these two operations the basic logical elements "and" and "or" were shown to be possible, along with other more complex logical functions from which can be built all logical operation. The entire discussion was in terms of binary computation, although it can be generalized to *n*-valued logic. An added attraction of majority logic is that the function of an aggregate of elements can be changed by processes implicit in the programming. For example, an "or" circuit becomes an "and" circuit by shifting the phase of the permanent source or, equally, by biasing the specific majority circuit with the output of another element involved in the computation. This provides great flexibility.

(b) (3)-P.L. 86-36 [redacted]



A_1	A_2	A_3	A_4
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

Fig. 17.

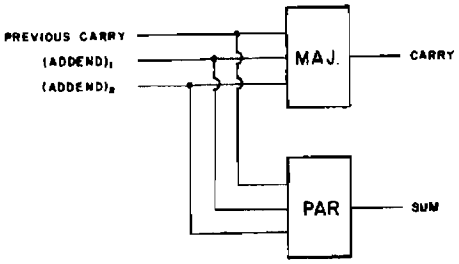


Fig. 18.

SOME PRACTICAL CONSIDERATIONS

A typical sequence of events in a signal channel is illustrated in Fig. 19.

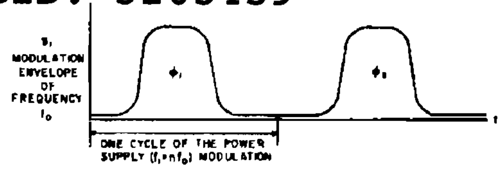


Fig. 19.

This shows a peculiar type of AM-phase-modulated sine wave. Information is represented by phase states Φ_1 and Φ_2, which may be the same or different. The AM has no purpose in the logical processing, and so may be used to monitor the operation of the machine and, in servo-control circuits, to maintain signal levels at the proper average. The phase reference of the entire machine is the phase of the master oscillator supplying or controlling the power-supply signals for each element. The modulation of the power supply determines the basic logical time-cycle.

The modulation envelope of the power supply has been assumed to have time variations that are slow compared to the periods of both f_0 and f_1. To give a numerical example, let the period of the power supply modulation be 50 cycles of f_1 (25 cycles of f_0) in a binary circuit. Reasonable values of f_1 and f_0 are 20 Kmc and 10 Kmc, respectively. The basic computing cycle has therefore, a period of 2.5 mμsec or a clock rate of 400 Mc. The envelope of the modulation of both frequencies is not sinusoidal, but good rectangular pulses are not required. Three harmonics would be sufficient. Thus the modulation envelope would involve frequencies of 400–1200 Mc.

To achieve a computing period of 1 mμsec (a "clock rate" of 1000 Mc) with the above time ratios would require f_0 = 25 Kmc and f_1 = 50 Kmc. The modulation envelopes would contain frequency components between 1000 and 3000 Mc. For an absolute bandwidth of 2000 Mc, this would be 4% and 8% relative bandwidth at f_1 and f_0, respectively.

Hardware realization of this scheme may well seem outrageous to computer-systems engineers who now are in the transistor age. And it would truly be outrageous in size, cost, and power, with conventional waveguide components at X-band (8.6–12.4 Kmc) and below. The techniques worked out with these conventional, readily available components can be applied to more practical geometries at higher frequencies. Higher frequencies of course have bad characteristics, such as high transmission attenuation, extreme precision requirements, and the lack, at present, of a complete line of components. These are things that must be overcome.

Von Neumann, who played the leading role in the birth of the modern electronic computing machine, has, in these ideas, made another great contribution to the field. Whether this contribution will have as much importance as his original efforts can be decided only after the technology for implementing the sub-harmonic response scheme has been more fully worked out. At this point the prospects look good.

Author's note—The Japanese have developed a sub-harmonic oscillator computer based on nonlinear inductance which uses the same phase script for information representation and majority logic schemes as represented in the von Neumann ideas described in this paper[9]. The basic circuit, called the Parametron, uses RF frequencies of 1 and 2 Mc and has a computing rate of 10 Kc. These two efforts are almost identical in concept, although far different in the speed of the suggested implementation, and from available records they seem to have been proposed in the same year, namely 1954, but there is no known direct connection between them.

(b)(3)-P.L. 86-36

[9] Saburo Muroga, "Elementary Principle of Parametron and Its Application to Digital Computers," *Datamation*, Vol. 4, No. 5, pp 31-34; Sept/Oct 1958.

About NSA

BY J. R. KILLIAN, JR.

~~Top Secret Eider~~

Address by J. R. Killian, Jr., November 3, 1958 at the National Security Agency, Fort Meade, Maryland.

General Samford, Ladies and Gentlemen—I am very grateful for this opportunity to visit with you of NSA today. It is always a thrilling experience, I'm sure, for anyone to come to an establishment of this kind and see it in its great scale, its great complexity, for the first time. Actually, this is not quite my first visit, because I had another visit several years ago with another part of your establishment, so I can use a story of mine about the young lady who went to a cocktail party, and after she had had two cocktails she went up to her hostess and she said, "You know, I feel a lot more like I do now than when I came in." -and so I do about NSA.

Now my first contact with NSA came back in 1954, I think it was, when I had the responsibility of directing a study, the report of which came to be tagged unhappily with my name. A group of scientists and engineers who participated in this study became, as a result of their participation, intensely and creatively interested in various aspects of our intelligence problems, and in the application of science to these problems. It was out of this study that there subsequently developed, I think it's fair to say, a whole new set of relationships between the intelligence community and particularly NSA and the scientific community. It was really out of this special activity that my own interest in intelligence matters was created and my present relationship with the intelligence community, which I find so stimulating and important, actually grew. I suspect, too, that it was because of this that I became involved as a member of the President's Board of Consultants on Foreign Intelligence Activities when it was created in 1956. Out of this combination of activities there has grown a new appreciation at the top levels of Government of the value of a close relationship between science and intelligence, and I see very real evidence that this understanding exists at the present time.

Just a year ago, two events occurred which both symbolically and in actual effect have demonstrated the new acceptance of the importance of science in Government affairs and which have relevance to your activities. These events included the reconstitution of the President's Science Advisory Committee in the White House, with an intensification of its work, and the establishment of my office as Special Assistant to the President for Science and Technology. In revitalizing the Science Advisory Committee, widening its scope and associating it with the White House, the President has given special recognition to the fact that science and technology, in addition to their use in solving specific problems, have a direct and creative impact on the formulation of Government policy

My function and that of the Science Advisory Committee is to provide answers to questions raised by the President, to undertake assignments for him of an advisory kind, to mobilize the best scientific advice of the country, and to make recommendations to the President on ways in which U. S. science and technology can be advanced, especially in regard to ways that they can be advanced by the Federal Government and how they best serve the nation's security and welfare.

It is important to note that the Special Assistant is invited to sit in on the meetings of the National Security Council and the Cabinet and, when appropriate or requested, to present the views and findings of the Science Advisory Committee. The President has thus created a mechanism to bring objective scientific and engineering advice to the top level of Government in a manner that reaches all agencies and departments of Government and yet can serve each of them.

In carrying on its work for the President, the Science Advisory Committee is organized into some fifteen panels at the present time, these panels including both regular committee members and members drawn from outside of the Committee.

In recruiting these panels, the policy has been to select the best-qualified scientists and engineers we can find in the country, and to draw upon their special competence and experience in tackling the problems confronting us. A number of these panels deal, of course, in the area of defense, but others are concerned with unclassified problems of importance to the advancement of science generally in the United States. We have a very active panel, for example, on Science and Foreign Relations; another on National Research Policy; and another which has just completed its work on ways of better handling the translating, abstracting, and dissemination of information. We have also set up *ad hoc* groups to try to help devise a national policy on high-energy accelerators. We have had active groups working on technical analyses to back up our international discussions on test cessation and on reducing the hazards of surprise attack.

The Science Advisory Committee serves as a board of directors or consultants to me as Special Assistant to the President. It has the prerogative, when it chooses, to report directly to the President. At the present time the Committee and my office have over fifty scientists and engineers at work.

Intelligence has been one of the principal interests of my office and of the Committee and one of the most active panels is the so-called Baker Panel. Dr. Baker is with us here today. This panel originally came into being as a result of a discussion in the President's Board of Consultants on Foreign Intelligence Activities, when representatives of NSA indicated that they would welcome suggestions on how some of their ideas might be implemented, in the research field particularly. The Board of Consultants recommended to the President that a carefully selected group of scientists be brought together, and he asked the Science Advisory Committee to select this panel and to be its sponsor.

I venture this bit of history by way of emphasizing the increased role of science and technology in Government and the key emphasis which groups of scientists that have been brought together by the President have placed upon signals intelligence. There is a clear recognition on the part of our policymakers of the unique scientific and technological requirements of signals intelligence and of the key role of the NSA in applying science to intelligence and to our national security.

It is not inappropriate to point out that the interest of the President's Board of Consultants on Foreign Intelligence Activities, his Science Advisory Committee, and the Baker Panel in the activities of NSA has served to emphasize the growing importance of the Agency and to increase the understanding at top levels of Government of its function, of the changing technology which affects its activities and scope, and of the impact of developing communications technology on the over-all organization of our signals intelligence activities. The recent revision by the National Security Council of a group of Intelligence Directives resulted from recommendations of the President's Board, and one of the new NSCID'S provides in consonance with the findings of the Baker Panel, as you doubtless know, for the consolidation under NSA of both COMINT and ELINT. The melding of these two great efforts reflects not only the fact that technology has inexorably made clear the interdependence of both COMINT and ELINT, but also the fact that NSA has increasingly demonstrated its capacity and effectiveness and shown that its remarkable resources and performance justify the taking on of these additional responsibilities.

I have had the illuminating and impressive experience of not only being interested in the technical aspects of NSA, but also of observing the results of its work as reflected in the reports at the National Security Council level. Week in and week out the information gathered through COMINT and ELINT reflects itself in the information placed before the policymaking offices of Government and proves its great usefulness. I think it important that you be aware of the impact of your work and of the great part NSA-collected information plays in our policymaking today.

I would add one further observation. I am aware, together with many others, of the extraordinary response of the personnel of NSA to emergency demands in the recent past. For example, when a recent foreign crisis demanded drastic extension of area intelligence gathering, technical and operational members of this agency, we know, kept a 24-hour schedule daily, even sleeping in their working quarters, and produced immensely valuable information which had not previously been specified by priorities or demands. This kind of performance and dedication, I can assure you, is deeply appreciated. I venture the further observation that such dedicated performance, carried out with great energy and inspiration, reflects the fact that here in this NSA environment personnel are allowed to respond within a framework which permits them to use their judgment, their knowledge, and their abilities in a way that stimulates exceptional performance.

And now against this background of personal experience and interest let me venture some comments about some of the current and changing conditions and requirements which seem to me to affect the role of the National Security Agency.

The United States policy of not initiating war, together with the present U. S. ability to retaliate if we are attacked, emphasizes the value to the enemy of achieving surprise. The ability of air attack and soon of missile attack to cripple, if not destroy, has greatly augmented the need of the U. S. to detect a surprise attack. It seems clear that no enemy would attack the United States under present conditions unless he thought that he had a chance of achieving surprise. Clearly the consequences of surprise are so great that every effort to eliminate it is justified. The hazard of surprise thermonuclear attack has greatly increased the importance and complexity of the classic mission of intelligence the provision of useful strategic warning.

A second factor that has imposed new requirements on information gathering and intelligence is of course the great compression of the time element as a result of the development of modern weapons systems. One need only note this effect by considering the problem of early warning when intercontinental ballistic missiles become operational. In the face of this condition we have no choice but to maintain a taut readiness and an alertness of response to assure that we have quick and certain reaction to any moves an enemy may make.

Still a third factor, in part affected by technological developments, is the increasing difficulty of gaining intelligence through more conventional and classical means and the consequent increased importance of new and sophisticated techniques. I need not tell you that we have obtained little information through classical covert operations inside the Soviet Union. No amount of skill or courage will serve to circumvent in any large degree the elaborate security measures available to a police state. I need not tell you either that changing technology in the communications field and in cryptography have made our information gathering more difficult. As a result of these conditions it has been necessary to place increasing reliance on advanced science and technology in our intelligence-gathering activities. In the subtle and complex art of measures and counter-measures in intelligence collection, it has become increasingly important that we use the ultimate in science and technology to improve our intelligence gathering. The challenge, in fact, which faces us today is to devise techniques which may be so close to the frontier of scientific knowledge that they may remain as a consequence unsuspected by the enemy for months or even for years and thus yield us an advantage because they are cloaked in the best of all possible security—the condition where we know more and are more advanced than the opposition.

Still another new condition which greatly affects NSA is the rapidly growing volume of electronic intelligence. The development of missiles and the great increase of telemetered weapons and space-vehicle activities are examples of the systems that generate growing volumes of ELINT and have the effect of broadening NSA's responsibility.

Yet another factor is the change in the nature of the race between cryptography and cryptanalysis. It would seem that the rate of breaking has now possibly been exceeded by the rate of making. This fact holds profound implications for the Agency. Especially does it point up the enormous importance of consolidated effort and teamwork and research and of the clear recognition of priorities in relation to achievable goals. There is no evidence at all that some of the most challenging NSA jobs such as [redacted] will be achieved by splitting up or separating in any way the NSA effort. Further, there is little evidence that these challenging jobs will get done as they might have been done in the past by some inspired splinter efforts or by groups going off to do something entirely different. The reading of communications information is just that and admits no fanciful escapes from reality. It cannot be accomplished by establishing a space platform from which to analyze the spectrum of Mercury.

I have spoken of the inexorable effect of technological change on the program and the activities of NSA. This warrants additional emphasis, particularly that aspect of it which points up the crucial importance of technical intelligence work to the welfare of the nation. Major developments in our technology, in business, and industry, and indeed broadly in our culture will emphasize the growing importance of communications processing in the years ahead. For example, computers, communications theory, extensive broadcast and personal communications systems, the growing literacy in the world, and the

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 403
(b)(3)-P.L. 86-36

need for increased education by mass communication techniques—in general the whole complex of sensing and control by which society orders itself is now clearly overlapping the NSA orbit. This will be an overlap of high value and significance if the gifted people who are being increasingly attracted to these general information handling activities can discover and understand that they can make enormously valuable contributions through the NSA itself. There are other forces apparent today which are of great significance. It becomes increasingly clear that the critical needs of coming decades in our society may not be primarily the obvious ones such as materials or foods or energy resources; they may indeed be the means of better organizing and ordering our society, and this implies increasing need and reliance upon communications. We face great increases in air and sea traffic, and eventually space traffic, which will have to be regulated by communications. You already know, of course, of the immense communication nets such as the SAGE System and the techniques they suggest for handling air traffic problems. An essential factor in these great systems of communication, of travel, and of transportation will be checking schemes We have also the possibility of systems which may be designed for the ultimate control of armaments. This week a group is departing for Geneva to discuss with the Soviets the techniques of reducing the hazard of surprise attack; a discussion of experts on the problem of monitoring various ways of springing a surprise attack. While this may appear remote from your present-day activities, I am sure that you will readily agree that if and when agreements are made for monitoring systems either for nuclear tests or for the purpose of reducing the hazard of surprise attack, NSA will have a big part to play in the period during which such systems are operating.

The increased importance of space and space vehicles is opening up an entirely new vista for signals intelligence. The reconnaissance satellite is an obvious possibility in space technology. Such a device can most certainly carry signals-intelligence equipment. In the light of present-day experimentation with radio telescopes, we may well discover techniques of using these research tools as collectors, to some limited degree, of signals intelligence.

With all of these impending developments before us we may well conclude that the survival of our society may depend upon the sampling and cross-checking of communications and ELINT signals which all nations must increasingly use to organize and direct their activities. This, of course, is looking far ahead, since we know that at present there is the heavily pressing problem of getting the original communications themselves good enough to do an elementary job of serving the purposes of free world governments to increase stability, security, and understanding. But that job will certainly be done. As it is done the

importance of verifying, cross-checking, and otherwise processing information by means other than the obvious sender and receiver will become of increasing importance. This is a stirring vision, far beyond the classical concepts of COMINT and ELINT, but it is a surely evolving one. It means among other things that the NSA will face the requirements of gaining practice and experience in very large-scale, very complex information handling. The systems-engineering development which improves the intercept and collection as well as the elementary analysis of a huge bulk of material recently being acquired can have tremendous value for responsibilities which may come to the agency in the years ahead.

In conclusion, I would note some of the important steps which have recently been taken or impending which should be of direct assistance to NSA in meeting its current problems and future responsibilities. I think, for example, of the concept and establishment of the CRITIC system. One of the highly valuable attributes of signals intelligence is its ability to react rapidly to perturbations within the enemy's communications system. If, however, the information derived from this perturbation suffers long delays in transmission, we have not gained anything. If we are to rely upon signals intelligence as our prime source of early warning information, we must be sure that the material arrives where it can be used promptly. It does no good to warn the target after the missile has reached its destination. In the development of the CRITIC system there is a prospect of insuring that the required timely intelligence arrives in the hands of the President in time to be useful.

Another important development which I alluded to earlier is the integration of COMINT and ELINT. Each of these fields is important in its own right, but the melding of them into an integrated whole can yield information that up to this time has remained unexploited. It can also insure that we do not miss important information that otherwise has not been available to us. I am hopeful that this new approach will be useful in meeting some of the telemetry and data-processing problems that we are now facing.

I also feel that the research institute which is now projected should be of great value in augmenting the presently very effective research activities of the Agency. It can help, without in any way weakening security, to bring the Agency in closer contact with the creative civilian scientific community. It is hard to restrain enthusiasm for the possibilities of having effective contributions to the basic understanding of cryptology and cryptanalysis without at the same time having to bring these new contributors into possession of necessarily super-secret material. Occasionally, academic research has revealed new general levels of knowledge, new patterns of what science or technology could reasonably be expected to do, without tying results to doing a particular thing, such as breaking a particular code. The evolution of NSA has reached the point at which it can make excellent use of this aspect of academic work and the projected research institute should help to make this possible. The student of cryptanalysis and of information processing in such an institute can work hard and imaginatively on information processing, and in a way, year in and year out, that enables him not to feel constrained by immediate day-by-day requirements or demands. I do not mean to suggest that such a research institute should be or can be separated or isolated from the in-house research and technology of NSA. Rather it should primarily serve to assure that research on cryptanalysis will be introduced to the NSA environment itself and flourish there in greater measure even than it has already. For example, the proposed institute should provide an effective frame of reference for the scientific achievements that must be appreciated in the vast NSA program in which achievement so generally means production.

These random observations, Ladies and Gentlemen, are prompted by the work of my scientific associates who have been devoted to the program, the people, and the objectives of NSA. They arise, too, from the opportunities which I have had through various bodies of an advisory kind, to look at the broad policy questions which are related to our national intelligence effort and to the science and technology which must so closely be coupled with this effort. What NSA is doing and what our entire intelligence community is doing is of enormous importance to our national security and our national leadership and as such it warrants the attention, the understanding, and the best efforts of able men and women who have contributions to make to its program. I feel this very strongly and I, in closing, would like to say again how much I appreciate your hospitality and to assure you that while you may, due to the wraps of security, feel that you work in obscurity, the importance of what you do and the fine spirit and dedication with which you do it are understood and deeply appreciated and are one of the great assets of our nation today in a time of trouble. And I would say finally how much we can all respect and appreciate and understand the fine leadership which this Agency has at the present time.

Thank you very much.

Data Transmission Over Telephone Circuits

BY [redacted]

(b)(3)-P.L. 86-36

Unclassified

Many of the higher-speed cryptographic machines developed at NSA are required to operate over telephone channels. Because the telephone plant was not designed for digital devices, data transmission equipments are often used as intermediaries between these machines and the transmission medium. This article reviews the fundamentals of digital signals, describes the problems involved in transmitting digital data over telephone circuits, and presents some of the data-transmission techniques employed in COMSEC equipments.

INTRODUCTION

Digital data in binary form is perhaps the simplest and most rugged language for electronic machines from the standpoint both of processing and of relaying information. Samuel Morse first used it in 1832 with the hand telegraph, and it has since been extended to machine telegraphy, the dial pulses in telephony, and more recently to digital computers, telemetry, and secure communication systems. Since Morse slowly hand-keyed "What God hath wrought . . ." over a forty-mile wire line, high-speed data has spanned continents and oceans by radio and telephone. Yet basically little has changed in the interim except the "keying" rate and the communication facilities.

The problems involved in transmitting electrical signals over telephone circuits for any distance are essentially these: the channel favors certain of the various frequency components which in combination constitute a signal in such a way that some arrive at the destination sooner than others, and all are not equally attenuated; and the signal may be further corrupted by noise picked up in transit. These difficulties affect voice and digital signals alike, but the ear is oblivious to the delay variations and tolerant to some extent of the other two. With high-speed data, however, all these factors--but especially delay distortion—have to be carefully considered.

GENERALIZED DIGITAL COMMUNICATION SYSTEM

A generalized digital communication system is shown in Fig. 1. The "raw" information fed to the input processor could conceivably be temperature fluctuations or speech. These are converted by the input processor into a series of discrete pulses, arbitrarily called the "message." The transmitter portion of the transmission equipment suit-

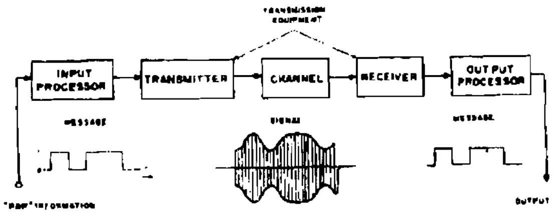


Fig. 1.

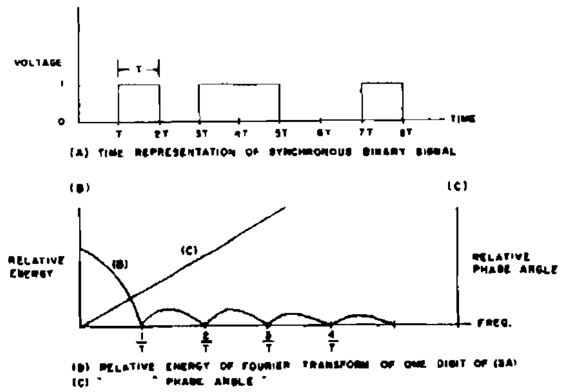
ably processes the message for transmission over the channel. Because of noise and the transmissive properties of the channel, the received message may not necessarily be that which was sent. The receiver portion of the equipment operates on the incoming signal in such a way as to minimize the disruptive effects of the channel and presents a replica of the message to the output processor. [1]

The two ends of the chain (the input and output processors) have been discussed in a previous article in the *Journal* [2]; we shall deal here with the properties of the parts between—the transmission equipment and the channel.

DIGITAL SIGNALS: FUNDAMENTAL CONSIDERATIONS

Digital signals represent information by a sequence in time of discrete symbols or signaling elements. Each signaling element is a choice from a finite set of alternatives. The simplest embodiment of a digital signal is one offering a choice between two possibilities for each signaling element: the binary signal. With a ternary signal there are three such possibilities; with a quaternary, four; and so on. If the transitions from one state to another only occur at prescribed time intervals the signal is *synchronous* or *time-quantized*. Signaling elements may be represented by the magnitude of a current pulse (telegraphy), the frequency of a sub-carrier frequency (Frequency-Shift-Key Telegraphy), the relative phase of a sub-carrier frequency (Collins Kineplex) [3], the position or duration of a pulse (Pulse Position or Pulse Duration Modulation) or a combination of the above.

One common message format, called *baseband*, is shown in Fig. 2a. It consists of a synchronous stream of binary elements of equal duration, with no intervals between them. In this case we say that the signaling element has a 100% duty factor; i. e., the product of the pulse duration by the pulse repetition frequency (PRF) is unity. The stream shown below would be described as a synchronous quaternary signal of 33%-duty-factor pulses.



(A) TIME REPRESENTATION OF SYNCHRONOUS BINARY SIGNAL

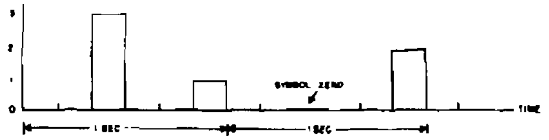
(B) RELATIVE ENERGY OF FOURIER TRANSFORM OF ONE DIGIT OF (3A)
(C) " " PHASE ANGLE "

Fig. 2.

A standard measuring unit of signaling speed or modulation rate that will apply to any of the possible digital signals is sorely needed by the data community. For digital data the *baud*, borrowed from telegraphy, is probably the one most widely employed. It is defined as being equal to the reciprocal of the shortest signaling element's duration (in seconds). A speed of one baud is therefore one element per second, but one element per second is not necessarily one baud. The unit *bits/sec* is also often used, although, as defined by Shannon [1] it is a unit of information, measuring the *entropy* (uncertainty) of an information source or the capacity of a channel [4]. When denoting speed, bits/sec can be defined as the product of the number of binary choices or bits per symbol by the number of symbols per second. To illustrate an ambiguity that often arises when these units are employed indiscriminately, let us refer to the quaternary signal sketched over-leaf. Here the modulation rate is six baud, or four bits/sec —assuming all choices to be equally probable—, or two symbols/sec. Only in the baseband case are bauds, bits/sec, and symbols/sec synonymous.

From the examples, we note that speed expressed in baud may not always convey what a system is doing, but rather indicates its maximum capability and so can be directly related to the bandwidth re-

(b)(3)-P.L. 86-36 [redacted]



quirements of a channel—which is doubtless the reason why it is preferred by communicators. Bits/sec. on the other hand, if properly applied, is a truer measure of actual performance.

From now on, we shall consider only synchronous binary signals, and express speed in bauds. It is, of course, true that many data systems are not binary or even time-synchronous—for instance, the Start-Stop Teletype but the simplicity and the prevalence of the case chosen make it peculiarly suitable for elementary discussion.

In the foregoing, the message has been represented as a time function[1]; to evaluate the effects or requirements of the transmission medium, however, it becomes necessary to express the message characteristics in the parameters of the medium. These are generally given in terms of the circuit's steady-state loss and phase characteristics; i. e., how the telephone circuit attenuates sinusoidal signals of various frequencies and how it affects their transmission velocities. The former is called the amplitude or frequency-response of the circuit and the latter the delay or phase-response.

Through Fourier-transform calculus we can describe each signaling element of Fig. 2a. as the sum of an infinite number of sine waves of various periods ($2\pi/\omega_n$), amplitudes (A_n), and initial phases angles (ϕ_n). Or by the same token the entire message may be transformed into a series of sine waves.[2] With the signaling element so represented, we may readily compare its frequency and phase characteristic with that of the channel on a common basis of A_n and ϕ_n. A plot of the A_n and ϕ_n versus frequency obtained by transforming one digit of Fig. 2a—is shown in Fig. 2b. The figures indicate that the bandwidth or frequency space of this signaling element extends to infinity and its phase characteristic is linear. But what is the minimum bandwidth needed to accommodate baseband at a speed of $1/T$ bauds?

Nyquist has proved that the minimum bandwidth needed for distortionless transmission at $1/T$ bauds is $1/2T$ cycles per second. He further showed that the frequency spectrum of baseband, if partitioned into bands $1/2T$ wide centered at multiples of $1/T$, contained the same information [5]. From any one of these "fundamental bands" the original signal could be uniquely recovered; recovery from n fundamental bands ($n = 2, 3 \ldots$) only yields a more exact replica of the signaling element. This gave telegraphers of 1928 and the present-day data transmission engineers an important criterion as to the minimum bandwidth needed for distortionless transmission of digital signals.

TELEPHONE CIRCUITS AS DATA COMMUNICATION CHANNELS

Message-grade telephone circuits are currently being exploited almost exclusively for use as high-speed data channels; program circuits from 5 to 15 kc are available on a limited basis at premium tariffs, as are 48 kc, 240 kc, and video channels. We shall restrict ourselves, however, to the message-grade circuits, which consist of loaded and non-loaded 19, 22, 24, or 26 AWG cable, found in the local plant, a 4 kc channel in a cable carrier, and open wire lines—to name a few—combined in various and sundry proportions, plus the associated central-office equipment and line repeaters.

The majority of these facilities in the telephone plant have been in existence since long before the era of high-speed digital machines and, unfortunately, do not possess the characteristics needed for optimum data transmission. Modifications of the telephone plant that would improve its data performance would likewise help speech transmission, but would be economically unsound, considering the present preponderance of speech traffic and the very slight degree of improvement that would be achieved. For this reason data transmission equipment designers strive to pattern their systems to the existing plant. Considerable effort is now being expended in this area by the military establishment and by commercial firms. A much publicized data-transmission system is the Collins TE206 Data Transceiver, which is rated at 2400 bits per second over a normal 3 kc channel. This system is currently being field-tested on message-grade telephone circuits, but as of this writing no conclusive performance data are available.

The telephone-circuit channel characteristics that will be given primary attention in what follows are bandwidth, linear distortion, and noise; non-linear distortion and level control will already have been taken care of because of their importance in telephony.

[1] For Fig. 2a it is:

$$f(t) = H(t - T) - H(t - 2T) + H(t - 3T) - H(t - 5T) + H(t - 7t) - H(t - 8T)$$

Where $H(t - x) = \begin{cases} 0, & t < x \\ 1, & t \geq x \end{cases}$

[2] So that the message of Fig. 2a could also be written:

$$f(t) = A_0/2 + A_1 \sin(\omega_1 t + \phi_1) + A_2 \sin(2\omega_1 t + \phi_2) + \ldots A_n \sin(n\omega_1 t + \phi_n),$$

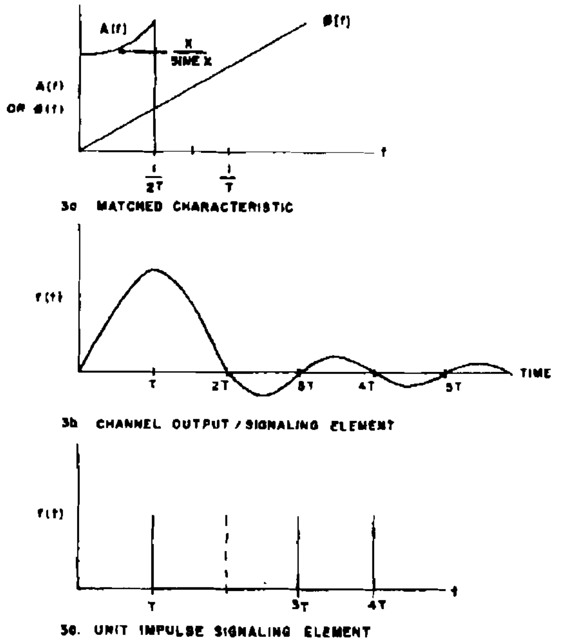
where: $\omega_1 = 2\pi/KT$, KT being the duration of the message,
A_n = amplitude of frequency $nf_1 = n\omega_1/2\pi$, $n = 1, 2, 3, \ldots$
ϕ_n = initial phase of frequency nf_1

(b)(3)-P.L. 86-36

[redacted]

Bandwidth Considerations

The bandwidth requirements of a digital signal were shown to be dependent on the modulation rate and on how faithful a replica of the signaling element was desired. To illustrate what happens when the bandwidth is reduced, let us consider the case of sending baseband at $1/T$ bauds over a channel $1/2T$ cycles in bandwidth. The channel, shown in Fig. 3a., is ideal, in that its frequency and phase response have been tailored to this signaling element. The channel output, per signaling element, has the form $(1/T)(\sin \pi t/T)(\pi t/T)$ and, as shown in Fig. 3b, is zero at integral multiples of T; successive inputs can occur only at integral multiples of T seconds— since the signal is synchronous— and will yield identical outputs. The received message will then consist of the sum of such waveforms.



3a MATCHED CHARACTERISTIC

3b CHANNEL OUTPUT / SIGNALING ELEMENT

3c. UNIT IMPULSE SIGNALING ELEMENT

Fig. 3.

If the channel output is examined or synchronously sampled at intervals of T seconds, the effect of all preceding inputs at the sampling instant for the pulse being considered is zero; furthermore, the signal is at its peak value, thereby maximizing the signal-to-noise ratio. Transmission at this rate over a channel of less bandwidth would result in intersymbol interference and thereby reduce the signal-to-noise ratio.

The choice of a different type of signaling element, e. g., a unit-impulse as shown in Fig. 3c, would not alter the output signal if the amplitude response of the channel were rectangular instead of skewed.

This constitutes an elementary proof that distortionless transmission in the Nyquist sense can be attained by signaling over a channel, matched to the signaling element, whose bandwidth is one-half the modulation rate. In practice, the characteristics of the ideal channel do not exist, and modulation rates less than one-half of the Nyquist maximum for a given channel bandwidth are used.

Linear Distortion Considerations

"Linear distortion" refers to both the delay and the amplitude distortion caused by a transmission facility whose amplitude and phase characteristics are not compatible with those of the transmitted signal, owing to imperfect filters and equalizers or to the fact that the effective bandwidth of the telephone circuit itself decreases with line length. Such departures cause the various frequency components of the signal to be unequally attenuated, and also to undergo unequal transmission delays. The net effect at a receiving terminal is "echoes"; i. e., the amplitude and zero crossing of the received signal are altered, thereby hindering the decision process, especially in the presence of noise. The correlation between echoes and the steady-state transmission characteristics was first published by H. A. Wheeler, and the reader is referred to his work [6] for a detailed presentation of this subject.

One way of undoing linear distortion is by performing the inverse process by means of a handicapping system of amplitude and delay equalizers that appropriately attenuate and delay each frequency component of the signal. This insures that the received component parts correctly combine in both amplitude and phase into the desired signal, by making the over-all delay and loss characteristics flat. Equalization in effect matches the channel to a particular signal. Very often, however, this may not offer the most practical solution: for example, baseband transmission over long distance telephone circuits is seldom feasible, because most of its energy is concentrated at the low frequencies, just where the channel characteristics, shown in Fig. 4, are

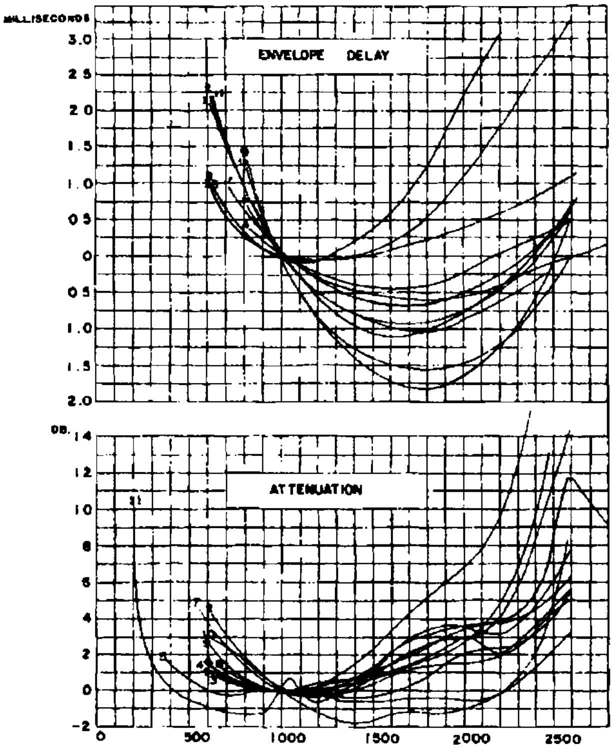


Fig. 4.

poorest. Equalizing below 700 cps, though possible, is impractical. But by frequency-translating a fundamental band of the signal to a more suitable position relative to the channel characteristic, using some modulation method,[3] we can readily overcome this difficulty. Even after modulation some equalization is generally required, but the amount is comparatively slight.

Noise Considerations

One definition of noise is that it is any extraneous fluctuation tending to interfere with the proper and easy perception of the signal. Noise in the over-all communications system comes from many different sources in varying degrees. The main types may be classed as *man-made, atmospheric,* and *thermal.*

Man-made noise covers a multitude of sins ranging from crosstalk to extraneous interference by auto ignitions. Atmospheric conditions, such as lightning and temperature-humidity variations, are nature's way of plaguing our efforts at communication by introducing noise impulses and diurnal changes into a circuit's frequency characteristics. Thermal noise is an inherent characteristic of all the components in the communications system from the wireline to the electronic hardware.

Man-made (dial pulses) and certain kinds of atmospheric noise share the qualities of abruptness and transience and are usually classed together as "impulse noise" by the communications engineer. Because of its nature, impulse noise defies mathematical analysis, so that most studies of it are empirical. If the signal spectrum it corrupts is narrow in comparison to the spectrum of the impulse, it resembles thermal or *white* noise in many respects. In any case, our attempt at providing an adequate defense against it leaves much to be desired. Thermal noise can be described, but in a probability sense only; for example, if all of the possible voltage levels of a thermal noise signal were plotted versus their relative frequency of occurrence, the resulting curve would be Gaussian with a mean value of zero, and the value of the second moment about the mean (variance) would be a measure of the noise power. In the case of synchronous binary signals, if the noise level exceeds half the peak-to-peak signal-level at the time of sampling, an error may result.

One obvious way to reduce the effects of noise and linear distortion introduced along the transmission path is to regenerate the signal before the damage becomes irreparable. In voice telephony, despite good repeater design, noise effects are cumulative, thereby limiting the number of tandem links, but synchronous binary signals can be

[3] A process which varies some parameter (amplitude, frequency, or phase) of a character frequency, in accordance with the information.

regenerated without error if the total perturbation never exceeds half the peak-to-peak signal amplitude; all that is required is a binary decision and a retransmission of a given waveform. Since the noise-level limits cannot be guaranteed, errors may occur despite regeneration, and will increase monotonically with the number of links in tandem. The error rate, however, will be considerably lower than in the nonregenerative case. But unless such regenerative repeaters could be provided by the telephone company they would be of little value.

Timing Considerations

As has been previously implied, timing is an important factor in the decision process at a regenerative repeater or receiver. This was illustrated previously in the example of binary signaling through a minimum bandwidth "matched channel;" in the case of linear distortion with the resulting echoes or "crossover jitter," accurate timing is even more essential because sampling margin is decreased. Timing plays an additional role in on-line additive-key cryptosystems because synchronous operation of remote key generators during the absence of incoming signals must be maintained. Both these considerations could be satisfied by extremely accurate clocks (timing sources) at the transmitter and the receiver, which after initial alignment would run synchronously for the cryptoperiod. Such devices are at present impractical because of their cost and size. Other schemes, which make use of the received message, have been successfully employed in COMSEC equipments. Three of these will be discussed.

One method used to maintain synchronism, called *time-base recovery*, derives the receiver timing by differentiating, rectifying, and filtering the received signaling elements. This is possible since synchronous elements inherently possess timing information. Such a means of frequency recovery is simply instrumented, but has the disadvantage that signal failure or long periods of steady mark or space will defeat it[4] Although the latter condition is very improbable in cryptographic transmission, the former is common in HF radio transmission during severe fading. The effectiveness of time-base recovery is dependent on the "memory time" or "Q" of the timing-recovery circuitry and the stability of the transmitter clock. Time-base recovery is used in ciphertext autokey systems which are self-synchronous cryptographically, and in additive-key systems where "crypto-synchrony" is established on a push-to-talk basis, so that long term frequency stability is not required.

[4] An even more direct and flexible means of time-base recovery is possible with a synchronous AM signaling element called "Dipulse" (described in the next section). Here the receiver timing can be derived directly by limiting the signal.

A second means of synchronization employs a local timing source in each repeater and the receiver. This consists of an accurate clock which is automatically phased or synchronized by the incoming signal. Recovery systems of this type can maintain system synchronism for relatively long periods in cases of signal loss, but are more expensive to instrument.

A third method transmits the timing information on a separate channel simultaneously with the normal output signal. Although it simplifies the receiver, it is costly from a transmission bandwidth and power standpoint. The last two methods are common in cases where synchrony must be maintained for the cryptoperiod.

TRANSMISSION TECHNIQUES

The data transmission techniques used in COMSEC equipments may be divided into two broad categories: time-division modulation (TDM) or serial methods and frequency-division modulation (FDM) or parallel methods. For most of the applications within the telephone plant, TDM suffices and is the choice on the basis of terminal-equipment size and economy, whereas FDM equipments are used for high frequency radio applications and are larger and more expensive [7].

TDM

Various time-division techniques are used for the transmission of binary data over telephone circuits, the selection being dependent on signaling speed and the particular transmission facility. Some of these preponderantly used in COMSEC systems, with speeds ranging from 1500 to 50,000 bauds, will be described.below.

Baseband Transmission

As the name implies, this refers to direct transmission of binary pulses over the telephone circuit. Baseband transmission in the 25-50 kilobaud range is possible on non-loaded cable pairs at distances up to 20 miles without regeneration. Here the channel characteristics can be made substantially compatible with those of the baseband signal by the use, above 3 kc, of simple amplitude equalization to offset the slowly falling channel response. Although the channel greatly attenuates frequencies below 300 cps, the resulting linear distortion is negligible at these speeds, because such a small percentage of the signal energy is affected.

Synchronous Amplitude Modulation

A common method of synchronous amplitude modulation, by which the signal is frequency-translated to match the channel, utilized in COMSEC systems, is "dipulse"; its signaling element and spectrum are illustrated in Fig. 5. In this technique, the baseband signal amplitude

(b)(3)-P.L. 86-36 [redacted]

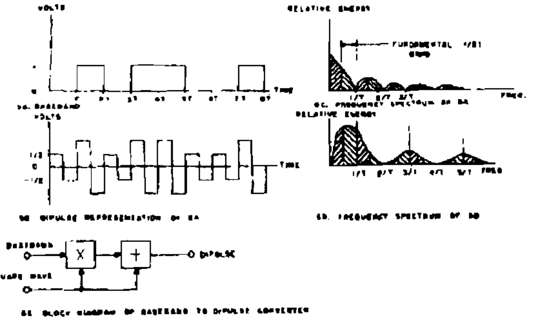

VOLTS
TIME
5A. BASEBAND
RELATIVE ENERGY
FUNDAMENTAL BAND
1/T 2/T 3/T
FREQ.
5C. FREQUENCY SPECTRUM OF 5A
VOLTS
1/2
0
-1/2
TIME
5B. DIPULSE REPRESENTATION OF 5A
RELATIVE ENERGY
1/T 2/T 3/T 4/T 5/T FREQ.
5D. FREQUENCY SPECTRUM OF 5B
BASEBAND
X
+
DIPULSE
SQUARE WAVE
5E. BLOCK DIAGRAM OF BASEBAND TO DIPULSE CONVERTER

Fig. 5.

modulates a synchronous carrier whose frequency is equal to the modulation rate. At the receiver the baseband can be recovered by a conventional AM envelope detector, and since timing information is always present in the form of a synchronous carrier, it can easily be extracted, as noted earlier. Although this technique requires about twice as much channel bandwidth as the baseband case, its frequency translation properties make it desirable on circuits having adequate bandwidth but a poor low-frequency response.

Synchronous Phase Modulation

An embodiment of phase modulation termed "diphase" is also used when the low frequency response of the circuit is not suitable for baseband transmission, and offers somewhat the same advantage as dipulse in regard to frequency recovery. In diphase the basic signaling element is one cycle of a synchronous carrier frequency that is equal to the modulation rate, whose phase is varied 180° in accordance with mark-space information of the message. The salient features of diphase are illustrated in Fig. 6. Here we note that its spectrum resembles that of dipulse, except that the carrier is suppressed.

Baseband, dipulse, and diphase techniques have been successfully applied to COMSEC equipments operating up to 50 kilobauds.

Vestigial Sideband

Vestigial sideband transmission, proposed originally by Nyquist [5], offers the advantages of frequency translation in fitting the signal to the channel at a small (as compared to dipulse and diphase) bandwidth price, but at the expense of vulnerability to noise.[8] Although both dipulse and diphase signals are in a sense frequency-translated versions of the baseband signal, the amount of translation is governed by the signaling rate, and may not optimally match the signal to the channel. This is not the case with vestigial sideband.

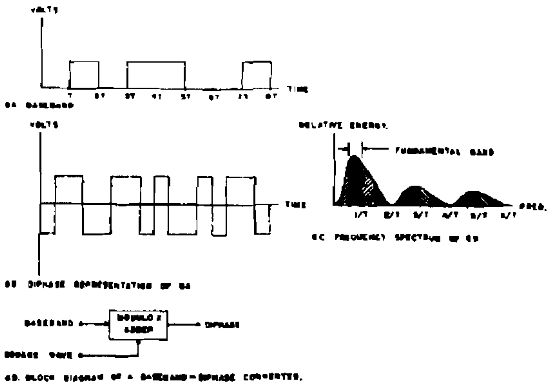


Fig. 6.

A vestigial sideband signal consists of one sideband of a normal AM signal plus a modified version of the other, with the carrier frequency so selected that the signal is translated to the linear portion of the channel characteristic.[a] (To clarify the bandwidths implied; if a fundamental band requires one unit, AM will require two units but VSB only about 1.15.) The various stages of vestigial sideband generation are shown in Fig. 7. As indicated, the baseband signal is first pre-shaped to limit its frequency-spread before modulation. The baseband is recovered by conventional AM detection.

FDM

Frequency division modulation entails more than the frequency multiplexing used in carrier telephony and teletype. The latter is simply a device by which many messages are channelized or "stacked" in frequency for transmission purposes, whereas FDM is a method used to combat delay distortion encountered in HF radio and wire-line transmission of high-speed data. In FDM a serial binary stream is converted to many slower-speed parallel streams, which in turn are frequency-division multiplexed. If an input message at r bauds is

[a] The picture portion of a broadcast television signal is a common example of a vestigial-sideband transmission

(b) (3)-P.L. 86-36 [redacted]

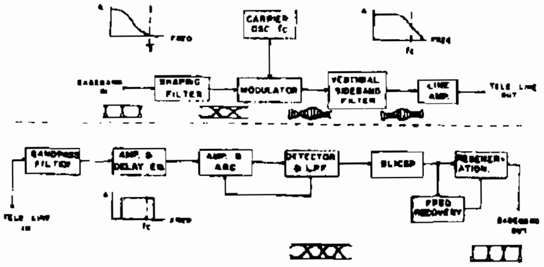


Fig. 7.

converted to n parallel streams, the modulation rate per transmission channel in FDM is then $R = r/n$ bauds. Since the modulation rate per channel is low if n is large, the effect of echoes due to linear distortion or multipath is less pronounced, but the narrow band channels require good frequency stability and level control in both the terminal equipment and the transmission facility in order to prevent crosstalk and intermodulation distortion.

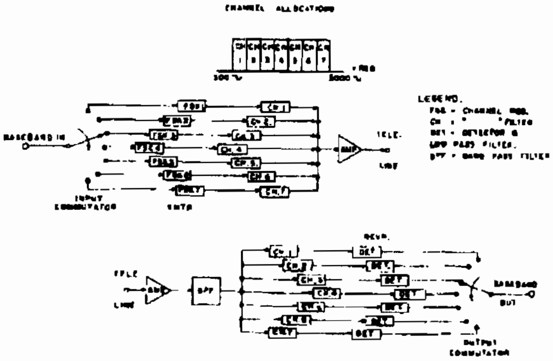


Fig. 8.

A typical FDM system is shown in Fig. 8. The message is time-demultiplexed by the input commutator, and each of the derived channels excites a frequency-shift oscillator in the voice frequency band such that a "mark" and a "space" correspond to oscillations of frequency f_{m_1} and f_{s_1} respectively (where the numerical subscripts denote the channel frequencies which are spaced throughout the voice band at intervals of 200 cps). The FSK outputs are linearly added for transmission, and the receiver performs the reverse process.

Frequency division modulation techniques have been successfully used in COMSEC systems at 1500 bauds over existing message-grade circuits in the telephone plant. For "attended" operation their salient advantages over TDM are decreased vulnerability to delay distortion and to noise, although this may be offset somewhat by crosstalk due to intermodulation distortion and system alignment.

CONCLUSIONS

The ideal data-transmission preparation equipment, neglecting considerations of cost, should be a flexible device that periodically scans the channel and selects the optimum transmission technique to match it. Until the advent of such a device, reliable data transmission over message-grade circuits on a random-call basis in the existing telephone plant appears to be limited to about 1000 bauds; higher-speed systems will require special circuits at higher tariffs. High capacity FDM transmission systems for use on voice circuits, though available, are not a panacea, because they are not readily compatible with serial-data processing systems, and are costly. Serial transmission techniques such as vestigial sideband, on the other hand, are economical and directly compatible with serial-data processing systems. The advent of low-cost high-speed data channels will certainly make them highly competitive.

In conclusion the author desires to acknowledge his debt to Mr. E. A. Enriquez, whose unfinished draft of an article on this same subject he has consulted extensively and repeatedly.

BIBLIOGRAPHY

[1] C. E. Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal*, July 1948.

[2] [redacted] "The ABC of Ciphony," *NSA Technical Journal*, July 1956.

[3] M. L. Doelz and E. T. Heald, "Binary Data Transmission Techniques for Linear Systems," *Proceedings of the IRE*, May 1957, p. 656.

[4] [redacted] "Some Notes on Information Theory," *NSA Technical Journal*, Vol. IV, No. 1 (this issue).

[5] H. Nyquist, "Certain Topics in Telegraph Transmission Theory," *American Institute of Electrical Engineers*, Vol. 47, p. 617, April 1928.

[6] H. A. Wheeler, "The Interpretation of Amplitude and Phase Distortion in Terms of Paired Echoes," *Proceedings of the IRE*, June 1939.

[7] [redacted] and [redacted] "Ionospheric Propagation," *NSA Technical Journal*, Vol. III, No. 4, October 1958.

[8] S. Goldman, *Frequency Analysis, Modulation, and Noise*, McGraw-Hill, 1948, p. 167.

(b) (3)-P.L. 86-36

Antipodal Propagation

BY N. GERSON

~~*Confidential*~~

A discussion of the special considerations involved in the reception of a radio signal at a point antipodal to the transmitter.

INTRODUCTION

Probably everyone is acquainted with "whispering galleries." These are rooms which after construction (sometimes deliberately, sometimes accidentally) focus sound waves originating at some particular source to a second point. Many of these are well known. There is one, for instance, in the old State Capitol of Maryland in Annapolis; another in the U. S. Capitol, in Washington; and another in the Louvre in Paris. Probably the one best known in this country is that found in Statuary Hall in the old House of Representatives in Washington. The elliptical room, whose walls are fairly good reflectors for sound energy, has two foci, and a whisper at one is clearly audible at the other. However, should the speaker move even a foot from the focus and then shout, his voice will fail to carry and will not be heard at the other focus.

Something similar, of course, can be constructed for any type of wave motion. Signals radiating from one focus would converge at the second with but small attenuation.

In this connection it should be noted that natural whispering galleries are already in existence. One such gallery exists in principle for radio waves propagating between the ionosphere and the earth. The two foci are (a) the transmitter location itself, and (b) its antipode.

Although the actual case for the earth and its ionosphere is somewhat complicated, the conditions may be idealized as shown in Fig. 1. This diagram illustrates two concentric spheres, the inner one corresponding to the earth and the outer one to the ionic layer which reflects the radio wave in question. The outer surface of the inner sphere and the inner surface of the outer sphere will be taken as perfect specular reflectors. To simplify the treatment, the wavelength, λ, of the electromagnetic wave will be considered as much smaller than the separation of the spheres, z; i. e., $\lambda \ll z$.

The latter condition holds for both the HF and VHF bands. For example, the ionic layer allowing reflection may be the *E*, *F*1 or *F*2, which have altitudes of approximately 100 km, 200 km, and 300 km, respectively. When the wavelength is less than 1000 meters, the condition $\lambda \ll z$ holds, and ray tracing is valid.

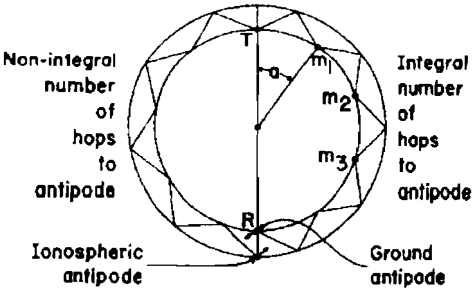

T
a
m_1
m_2
m_3
R
Non-integral number of hops to antipode
Integral number of hops to antipode
Ionospheric antipode
Ground antipode

FIG. 1.

Figure 1 represents a meridional cross-section through the spheres, containing the center of the spheres, the radiator T, and the antipodal point R. Two rays are illustrated, both of which are re-focussed at the source T after one transit around the inner sphere. The ray which completes this transit in an odd number of hops is reflected from the outer sphere at the antipodal distance, while the ray making an even number of hops, intersects the true antipode of the source.

Radio waves of the latter type are of great potential interest. They must satisfy the relationship

$$ma = \pi \tag{1}$$

where m is the number of hops to the antipode, and a is the central angle (at the center of the spheres) subtended by one hop. Obviously m must be a whole number.

It should be realized that Fig. 1 illustrates a cross-section through the spheres in *one* plane only. The same conditions occur in all planes passing through T and R. Thus the signal strength at the receiver is the intensity of all rays integrated through an azimuth of 360°, arriving at R. In the ideal case, this intensity is appreciable, and allows a clear, unambiguous interpretation of the signals radiated at the source.

Some comments may be made about those hops where

$$ma = 2\pi, \tag{2}$$

m being integral. (This condition includes not only those cases where rays are focussed at the ground antipode, but also those where they are focussed at the ionospheric antipode. In either event the rays again pass through the source of radiation, T, after one transit around the earth.) When Equation (2) is satisfied, the reflections m_1, m_2, etc., at the inner sphere are termed *multiple image points*.

At the multiple image locations, rays arrive only along the great circle path containing both the receiver and the source, some being propagated along the short segment and others along the long segment of this path.

In the ideal case considered above, the time difference, Δt, between the arrival time of (a) the short-segment and (b) the long-segment rays is constant along the small circles containing the loci of all points m_1, m_2, etc., respectively (see Fig. 2). Each of the small circles is centered on the axis T–R. For one global transit, the time separation, Δt, attains its maximum at T and its minimum at R. At T, $\Delta t = t_l - t_s = t_l$, for the short-segment wave arrives at time $t_s = 0$ seconds, and the long-segment ray arrives at $t = t_l$, the time required for one transit around the sphere. At the antipode R, the geometrical short- and long-segment paths become equal, whence the time difference $t = t_l - t_s = 0$.

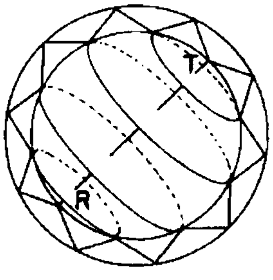


FIG. 2.

The time required for HF radio waves to make one transit around the globe has been measured on a great number of occasions and found to be fairly constant at $t = 0.13788$ seconds. The transit is made via a multihop propagation between the ionosphere and earth, as in the ideal case portrayed in Fig. 1.

The magnitude of the time separation between the long- and short-segment paths provides some indication of the fading expected at different locations. Severe fading would result when the two waves arrive sufficiently out of phase to produce destructive interference, with markedly distorted signals. Thus the least interference between the two signals may be found at the sites T and R. (The fading which occurs because of interference between the ordinary and extraordinary rays, lateral reflections to the receiver, and polarization, will not be considered here.)

Maximum fading between the signals of the long-and short-segment paths probably may be expected at first-hop distances from the antipode, where the time separation, Δt, is small, and the signal intensities are approximately equal. Appreciable fading would not be expected at the antipode, since all geometric paths from T are equal. In practice, however, the electrical paths to the antipode are of different lengths for different rays, because of differences in the dielectric constant, the presence of ionospheric discontinuities, differences between day and night paths, and so on.

Several interesting aspects of the ideal model may be noted. With two perfect, concentric, spherical reflectors, energy radiated from a source T is reflected indefinitely without loss. Thus, the entire volume between the two spheres may become uniformly filled with the radiated energy, which is confined without loss between the two spheres.

It should be noted that in Fig. 1, only one ray path was shown in the T-m_1-m_2-R plane. However, a number of rays may propagate from T to R provided an integral number of reflections takes place with each. For example, assume that Equation (1) is satisfied. If the central angle is now halved, the number of hops is doubled and, in general, $ma = 2m(a/2) = \ldots = (m\ n)\ (a/n) = \pi$. When no energy is lost or dissipated by the spherical reflectors, emissions at any frequency in the electromagnetic spectrum, radiated at angles satisfying Equation (3), arrive at the source T after one spherical transit. Any ray not arriving at T at the first transit will arrive there (approximately, if not exactly) at some later time.

As perfect specular reflectors are non-existent, the energy loss arising from multiple reflections within the two concentric reflectors should be examined. If the reflectance at each reflection point is r, the final intensity is given by

$$I = I_0\ (r)^m \tag{4}$$

where I is the final intensity; I_0, the initial intensity, and m the number of reflections since emission. An indication of the decrease in intensity for various values of reflectance and after a given number of reflections is given in Table 1.

THE IONOSPHERE AND THE EARTH

The actual ionosphere and earth depart from the simplified model described above. Although any particular ionic layer is not spherical, its average departure from sphericity (about 50 km in a radius of 6550 km) is about 0.7 per cent for the E, $F1$ and $F2$ regions. The ionic surface contains height, density and slope discontinuities, especially across the sunrise-sunset line, in the vicinity of the geomagnetic equator and in polar regions. A slope discontinuity, by changing the angle of incidence and reflection, will direct a ray away from an expected multiple image point, m_1.

TABLE I

Effective Reflectivity After Multiple Reflections*

n	Reflectivity			
	$r = 0.8$	$r = 0.9$	$r = 0.95$	$r = 0.99$
1	0.800	0.900	0.950	0.990
5	0.328	0.590	0.774	0.951
10	0.107	0.349	0.599	0.905
15	0.0352	0.206	0.465	0.860
20	0.0115	0.122	0.359	0.817
25	0.0038	0.072	0.277	0.778
30	0.0012	0.042	0.215	0.740
35	0.0004	0.025	0.166	0.704
40	0.0001	0.015	0.132	0.669

* $R_{eff} = r^n$, where: R_{eff} = effective reflectivity
r = reflectivity
n = number of reflections

Another discrepancy which may be important for antipodal radio wave propagation on the earth is the very low electron concentration existing in the winter polar ionosphere. Near the winter pole direct sunlight is absent for some months even at ionospheric altitudes. Under these conditions the electron density falls to low values, and the critical frequencies of the E- and F-layers become rather small. The outer sphere of the ideal model (Fig. 1) then contains a "circular hole" through which HF radiation may escape into space. The radius of the missing spherical zone on the earth is about 15° and represents about 2 per cent of the area of the ionosphere.

The effect of the ionospheric hole may be visualized from Fig. 3. With the outer sphere essentially missing within the winter polar circle, radio waves transmitted at the winter pole would escape directly into space. No ionospheric reflections would be possible, and the waves could be received only within the ground-wave, radio line-of-sight, and diffraction regions. Tangent HF rays from the transmitter would not encounter a reflective ionic layer. For a transmitter at the winter pole, transmitted HF energy can escape into space.

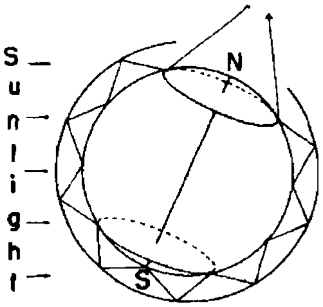


Fig. 3.

It should be noted that by the reverse of this mechanism, extra-terrestrial emissions either from natural or satellite transmitters may be channelled to the antipodal receiver.

If the transmitter were at the summer pole and the receiver at the winter pole, somewhat similar conditions would exist. In this case, all energy transmitted at an appropriate frequency could be successively reflected by multihop as the wave was propagated towards the winter pole. Near this pole, however, the lack of a reflecting region for HF radio waves would permit the energy to escape into space instead of being returned to the earth at the pole itself (see Fig. 3). It should be noted that the further the location of the transmitter and receiver from the winter pole, the smaller the fraction of energy escaping by this mechanism.

The preceding example represents an extreme. Most transmitters on earth are at considerable distances from the geographic poles. Thus, while the peculiarities of the polar ionosphere present some problems, they may not pose a major obstacle in antipodal propagation. While the winter polar ionosphere represents a hole in the HF reflector, the high latitude ionosphere during the equinoxes presents absorption problems. If equinoctial absorption occurs simultaneously in both polar regions, spring and fall may offer the greatest difficulty to antipodal propagation. In general, however, if a sufficient number of rays are directed to the antipode, adequate reception will be possible.

It should be recognized that with the ideal model, radiation at all wavelengths may be reflected. In practice, however, the normal diurnal variation of the ionosphere will limit the efficiency of propagation of different frequencies. These limitations arise from the daily variations in the electron concentration and in the altitude of the maximum electron density. In operating practice these variations may be roughly interpreted in terms of changes in the maximum and lowest usable frequencies, respectively. If at any particular ionospheric refraction point the operating frequency exceeds the local penetration frequency, a portion of the wave energy escapes. Similarly with absorption: if the operating frequency is locally absorbed, a portion of the wave energy is lost. If for the entire path sufficient energy penetrates the layers, the MUF is exceeded and the possibility of reception of the radiated energy is greatly reduced. Likewise, if for the entire path absorption is appreciable, the LUF has not been exceeded and reception of the radiated energy again becomes difficult.

In general, the ionosphere is inhomogeneous and anisotropic, both with respect to space and time. Its electron density at some locations or on some occasions may be low enough to allow energy from the incident ray to escape, either partially or completely, or to be absorbed. Whether this condition will negate successful antipodal propagation depends upon the fraction of energy lost or absorbed. Ultimately, of course, the occurrence of favorable periods is a function of season, time of day and portion of the solar cycle.

The initial model considered two concentric specular reflectors. For very low frequencies, where reflection may be considered to occur at the lower boundary of the *E* layer, this model probably describes actual propagation conditions. The outer reflector appears sufficiently smooth and regular everywhere except in the winter polar region. Thus, with VLF and LF, antipodal propagation possibilities are probably good throughout the 24-hour period, and during both winter and summer.

Consider a second model where the reflectivity of one hemisphere of the outer sphere differs from that of the other. The latter case better approximates the true characteristics of the earth and the ionosphere, where the day and night ionospheres have somewhat different properties.

This case applies more aptly to HF propagation where hemispheres having distinct reflectivities must be carefully considered. The ionospheric layers in the illuminated and the dark hemisphere differ not only in electron density but in altitude. In general, a variety of abnormalities in reflectivity occur, caused by: different ionic densities; abnormalities such as sporadic *E*, trans-equatorial *F*, and auroral ionization; different layer altitudes; different refractivity gradients; layer tilts; and so on.

Thus, for HF, the height of the reflector (external sphere) is different over the day and night hemispheres, while the twilight ionosphere may be considered as a transition zone between the two, with the result that the antipode for HF may not be a true optical focus, but rather an aberration.

Nonetheless, and in spite of these many potential difficulties, a number of isolated examples indicate that an antipode focus exists much more frequently than commonly thought. The potential of antipodal propagation for communication purposes is such as to warrant further investigation.

ROUND-THE-WORLD SIGNALS

A fair number of studies have been made on "round-the-world" propagation. These investigations were made on a comparison of the long- and short-segment great circle path signals emanating from a given transmitter.

Initial investigation by Quaek (1926), Quaek and Morgel (1926, 1927, 1929), Eckersley (1927) and Taylor and Young (1928) were devoted mainly to determining the time interval, *t*, elapsing between the reception of the short- and long-segment radiations. The results indicated discrepancies in Δt exceeding 5 per cent. However, careful examinations with more refined equipment later indicated that Δt had a constancy within 0.004 seconds (Hess, 1948, 1949).

The early experiments prompted von Schmidt to undertake (1934-1936) a theoretical analysis of propagation in the spherical shell existing between two concentric spheres. He formulated the sliding-wave hypothesis of ionospheric propagation to clarify the observations. In von Schmidt's (1936) sliding-wave theory, the transmitted wave propagates along the lower boundary of an ionospheric limiting surface. Just as a ground wave travels with constant velocity along the ground, the sliding wave was assumed to travel as a surface wave along the lower surface of the ionosphere. This wave radiated continuously, and at a definite angle, from the ionosphere to the earth.

Von Schmidt's theory was in contrast to the multiple-reflection theory which ultimately superseded it (Hamburger and Rawer, 1947; Lassen, 1948). The latter merely represented a multihop path between the ionosphere and earth as shown in Fig. 1. While both theories were current, a series of practice observations was initiated in Germany to determine which hypothesis could best clarify the observations. The investigations provided very accurate values of Δt. From these measurements, it was found that the distance between the transmitter and receiver could be obtained with accuracies of ±25 km, provided that the separation between transmitter and receiver was at least 1000 km. The recordings also confirmed earlier results which indicated that HF signals could be detected at very distant receivers.

In the course of the observation, it was discovered that in addition to the short-segment and long-segment transmissions, signals which had made more than one transit around the earth were detectable. Several instances were found where signals were received after a third or fourth transit around the globe.

An indication of the size of the antipodal observation area has been given by various researchers. Whales (1956) predicted that the antipodal area could have a radius of about 500 km centered on the antipodal point. His conclusions were based on angle-of-arrival measurements. It was assumed that the ionosphere acts as a diffuse reflector, and that impinging rays may be deviated by angles of up to 0.5°, per reflection. Round (1925) considered that antipodal signals should be received within a radius of about 1000 km from the antipode; however, the results do not confirm the existence of such a large area. Guierre (1920) found that for very low frequencies signal strengths decrease at about 1000 km from the antipode.

Guierre studied field intensities of radio waves, radiated from Lyon, at the antipodal point near Chatham Island. Day and night intensities were practically identical. One test indicated that when the Lyon transmitter was received strongly at the antipode, a diminution in signal strength was observed up to about 800 km from the antipodal point. On another occasion a second intensity maximum was observed about 600 km from the antipode, while at the same time lower signal intensities were observed between the two sites. The effect may perhaps be explained as a multiple image formed one ground reflection away from the antipode.

Round and others (1920) noted that even within an area of about 1000 km from the antipode, fading could become sufficiently strong to make the signals unintelligible. However, when a directional antenna was employed, it was possible to reject the interfering signal (which arrived at an azimuth of close to 180° from the stronger signal) and thus noticeably improve the readability.

There are several possible mechanisms for causing the observed interference and fading. For a non-antipodal receiver, the superposition of radio rays arriving from both the short- and long-segment great-circle paths can add characters and, on occasion, make the signal completely unintelligible, particularly with high-speed messages.

Antipodal reception has been observed sporadically. Observation from Pyongtaek and Chunchow, Korea, in 1957 indicated that voice and CW were received from Brazil and from naval traffic in Brazilian waters. Reception generally was possible between 03–08 and 17–24 LST. In late 1956 and early 1957, tests at Seoul, Korea showed that reception of 100- to 200-meter radiations originating in South America was possible "every day or so." Generally, however, the tests were conducted for rather limited time periods.

ANTIPODAL PROPAGATION

Before discussing some general features to be expected in antipodal propagation, the identification of the antipode on earth might be mentioned. The location of antipodal pairs may quickly be discerned from the definitive relationships $\theta = \theta_a$, and $\theta' = 180° - \theta'_a$, where

θ = latitude (°N)
θ' = longitude (°W)
θ_a = antipodal latitude (°S)
θ'_a = antipodal longitude (°E)

In general, no large continents seem to be antipodal, a fact which may account for the lack of reports concerning this type of propagation.

The hours of reception of signals from the antipode require study. Many reports have been prepared regarding reception of radio waves over very long distances, but the stations studied were not strictly antipodal. The results clearly indicate that radio-wave radiations at distances of 10,000–15,000 km from the transmitter may be received without difficulty for about 4–6 hours daily. When the stations were more closely antipodal, reception was possible for 5–7 hours daily (Hess, 1938, 1939). Guierre (1920) reported 24-hour reception of the radiated transmissions from the antipodal point. Whether the reception occurred constantly or sporadically throughout the day is not known. It should also be noted that the antipodal image of Sputnik I was received on a number of transits; but the satellite constitutes a special case, (Wells, 1958; Manning, 1958), particularly for transmissions which occurred outside the ionosphere.

FADING

While fading, at times severe, has been known for some time in reception over very long distances, few reports indicate the presence of fading at the antipode. Fading over long paths may arise from interference between the short-segment and long-segment great circle waves at the receiver site.

At the antipode, where the geometrical paths are equal, fading may be produced by variations and fluctuations of the refractive indices along the path. This type of fading, however, would probably be extremely rapid, and minor in comparison with other propagation effects. Nevertheless, when extremely high-speed transmissions are involved, or if small phase shifts are to be measured, the small differences in electrical length of the various paths may be significant. Obviously, the employment of directive antennas oriented along the most favorable path will diminish or entirely remove any potential interference between the daylight and darkness rays.

Antipodal reception would not require the utilization of large, expensive antennas. Long wire, rhombic, and a variety of omnidirectional antennas have been utilized for very-long-distance propagation studies, and would be suitable for reception at the antipode. When fading caused by destructive interference between the day and night waves is severe, use of directional antennas will usually remove the fading and permit unambiguous reception of the desired signal.

While relatively few results are available on antipodal propagation, the few tests which have been undertaken indicate that omnidirectional antennas of relatively simple design are effective. In view of the paucity of data on this topic, however, a study of the comparative performance throughout the day of both omnidirectional and directional antennas is required.

Direction finding at very long distances has been attempted on many occasions. In general, the results seem to be characterized by a definite difficulty in choosing a bearing. At a frequency of 10 kc/s and at distances of about 19,000 km from the transmitter, tests have indicated (Namba, Iso and Ueno, 1931)[1] that the bearing angle is a function of the time of day. In this instance angles for the closely antipodal signal changed markedly with time. When the Monte Carlo transmitter was monitored at Tokyo (true bearing 90°) the DF reading showed an apparent arrival of the wave from the West (270°) during the morning. At about 1000 LST, no bearing could be measured. Later, the signal arrived from about 45°. The bearing then gradually veered eastward, passing through 90° and becoming 150° at local sunset. After sunset, measured DF values slowly returned to the true bearing of 90°.

The effect may be easily explained if it is accepted that the wave propagated principally in the dark hemisphere. Although Tokyo and Monte Carlo are not strictly antipodal, the change in bearing angle indicates that the direction of the strongest wave more or less followed the sun, and moved around the earth with the twilight, dark, and daylight zones.

[1] S. Namba, E. Iso, and S. Ueno, "Polarization of High Frequency Waves and Their Direction Finding." *Proc. I.R.E.*, Vol. 19, p. 2000, (1931)—Editor.

SUMMARY

Antipodal reception is clearly possible, since it has been observed in the past, at least for limited hours of the day. Further, on theoretical grounds its use as a standard procedure seems promising, although several comprehensive studies are needed. Thus, the number of hours per day during which reception is possible is not fully known, and it is uncertain whether omnidirectional or directional antennas (possibly rotated during the course of the day) are preferable; and whether fading or auroral absorption is in reality a difficulty. The investigations could indicate the potential of the method and possibly determine what antenna improvements would optimize the results.

From the preceding discussions, it is clear that in principle the antipodal focus may be utilized to receive signals (in the range 15 kc/s to perhaps 60 mc/s) radiated within the spherical shell bounded by the earth's surface and the ionosphere. In practice, however, the actual state of the bounding surfaces will influence the intensity of the refracted signal and the possibility of reception. Even if calculations are made, the anticipated signal strengths may depart appreciably from those later experienced.

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

FOIA Case: 51551B
20 February 2008

This is a final response to your Freedom of Information Act (FOIA) request of 30 September 2006 for 21 articles from the NSA Technical Journal, among them *Soviet Science and Technology: Present Levels and Future Prospects* (Vol. IV, No. 1, January 1959). As we explained in our letter of 11 January 2008, this document contained other government agencies' information and was referred to the appropriate agencies for review. That consultation process is now complete. Your request has been processed under the provisions of the FOIA, and the requested material is enclosed.

Sincerely,

PAMELA N. PHILLIPS
Chief
FOIA/PA Office

Encl:
a/s

Soviet Science and Technology: Present Levels and Future Prospects

BY A. SINKOV

~~[illegible]~~

Recently, there were discussions at the Agency Personnel Development Board of the work done by NSA personnel at the senior War Colleges. A question was raised whether term papers prepared at such schools might be suitable for publication in the Technical Journal. *It was generally agreed that where the subjects were of interest to NSA, such publication would on occasion be desirable*

As a result, I hunted up the term paper which I had prepared in 1954-55 when I was a student at the National War College. On rereading it from the point of view of timeliness, I felt that the lapse of three years had not significantly affected its content or conclusions. Certainly some parts of it could be rewritten and sharpened, but there is perhaps interest in reading it with the hindsight of the additional information of the intervening period. For this reason I have felt that it would be appropriate to submit it unchanged rather than to attempt to bring it up to date

I. INTRODUCTION

We are living in an age of science. The developments of science and technology during the past two generations have been of such breadth and of such magnitude as to overshadow human activity of all other kinds. The prominent position which the United States occupies today in world affairs stems directly from its technological capability just as that same capability was the prime factor to which we attribute our victories in the two world wars of this century. Considering how important science is, and considering that the Russians must assign to it the same position of importance, it is imperative that we keep as well informed as we can about the state of Soviet science.

The problem of doing so, however, is complicated by the behavior of the Communists: by their establishment of the Iron Curtain; by their secretiveness; by their restrictions on the movement of foreigners into and within their territory; by the strict control they manage to exercise over their own personnel abroad to prevent defections and disclosures; and by their methods of handling statistical information. These complications make it more difficult to acquire valid, properly interpretable data; they give rise to much speculation as to just what the picture is when only a few pieces of the jigsaw puzzle are in place and some of them blurred; they point up the inadequacies of our present intelligence and give rise to conflicting opinions. Nonetheless, there is considerable information available on which to form judgments. Let us examine the major sources of such information.

II. SOURCES OF INFORMATION

Open Literature

Under the heading of open literature there are included those sources of information which are openly disseminated, such as research journals, text books, occasional scientific articles in periodicals, and economic statistics. By a slight extension, we could also include those propaganda broadcasts which contain information bearing on science and technology. The main difference between these sources of information in the Soviet Union and elsewhere is that in the U. S. S. R., every bit of material is carefully scrutinized by government authorities, and only such items as are considered unclassified may be disseminated. Since the Russian standards of classification are much stricter than ours, a much smaller amount of material is thus permitted to get out.

At one time, most research papers in Soviet scientific journals carried abstracts in English and in French, but this practice has been discontinued.[1] The result is a reduction in usefulness to us, since the number of Western scientists who can read Russian is quite small. Although all universities in this country giving graduate degrees in science require candidates to demonstrate knowledge of two foreign languages, very few schools have included Russian as an admissible choice. A further point about this open literature is that some of it is printed in editions of limited number so that it is more difficult to get copies for use outside the Soviet Union.

Information obtained from CIA indicates how much scientific material is available From 1950 to 1954, 36 Soviet periodicals have been obtained for study; in some cases the files are complete, in others there are gaps and irregularities.[2] The approximate total number of volumes that have been received during this period has been constantly increasing from 180 in 1950 to 240 in 1953. (The figures for 1954 were not complete at the time this information was made available.)

The Soviet *Catalog of Periodicals and Journals for the Year 1955* lists four new periodicals that will shortly become available. It is of interest to note that one of these, about which there will be some comment on page 44, is entitled *Automatics and Telemechanics.* Scientific papers, monographs and information on special scientific fields are also included in general periodicals such as *Reports of the Academy of Sciences.* Almost complete files of these general periodicals are available for 1950 to 1954.

Clearly, the information derived from the research journals and monographs is of high validity. It gives indication of the number and quality of research personnel, and the technical level of the problems investigated. In those fields requiring special facilities for experiment, it can indicate the number and character of such facilities, their variety, and the quality of their equipment.

The information that comes from published statistics and from radio broadcasts is of a different order of validity and must be examined much more critically. The figures which are released are often open to question:[3] they are manipulated and exaggerated; they are seldom given in absolute terms—rather as percentage changes and rates of change; the basic indices of comparison are subject to modification (published figures being sometimes the planned rather than the actual figures); harvest data may be in gross rather than in net terms; and, in short, information of this kind needs careful evaluation before it can be considered meaningful and acceptable.

Manufactured Items.

A second important source of information about Russian technology is found in the analysis of manufactured equipment—military, industrial, and consumer items.

The most fruitful source of such information in recent times was equipment captured in Korea, which has been searchingly analyzed in order to gain information about the effectiveness of Russian technology. For example, the Air Technical Intelligence Center has published a large number of studies of captured equipment. In addition to such basic considerations as effectiveness of aircraft and armament, quality of fuels and lubricants, capacity of communications and electronics equipment, these studies investigate the materials used,—metals, rubber, plastics—the effectiveness of design, the adaptability to mass production, the ease of operation and maintenance, the inter-changeability of parts, and sometimes even provide information about the quantities that have been manufactured, as well as the location of the plant where this was done. So important was captured Soviet equipment as a source of information that it gave rise to a special operation in which the inducement of $100,000 was offered in propaganda broadcasts to any pilot who would fly a MIG-15 over to the U. N. forces. That this also turned out to be a master stroke of psychological warfare was an incidental result of the quest for technical intelligence.

[1] T. Dobzhansky, "Lysenko's Michurinist Genetics," *Bulletin of the Atomic Scientists,* Vol VIII, No. 2, February 1952, p. 43; J. R. Kline, *Soviet Mathematics Bull. of the Atomic Scientists* Vol. VIII, No. 2, February 1952, p. 46; E. Rabinowitch, *The Exchange of Scientific Information with the Soviet Union,* February 1953; p. 14.

[2] An interesting discussion of "The Exchange of Scientific Information with the Soviet Union," is given in *Bulletin of the Atomic Scientists,* February 1953, pp. 13 ff

[3] Harry Schwartz, *Russia's Soviet Economy,* Prentice Hall, 1954, p. 129.

Other items of Soviet equipment available for study are those that can be bought in the open market in the Soviet Union or in countries to which it exports manufactured items. They can be seen, for instance, at international fairs and expositions, where they may be displayed for propaganda purposes. Such exhibitions have been held in the last few years in Milan, Bombay, Beirut, Bangkok, and Leipzig.[1]

In both kinds of instances—captured as well as commercial equipment—the number of samples available is not very large. Besides, the equipment may be several years old and so does not necessarily reflect a current situation. Nonetheless, the findings are significant and permit objective judgments of Soviet technological capability.

Observers

First-hand information from people who have been in Russia is naturally desirable and important. These observers may be official representatives of the Free World in a diplomatic or scientific capacity; they may be visitors; or they may be defectors from the Soviet Union.

Among those from the Free World who have visited Russia and have been able to provide useful technical information are people like the following:

1. J. C. Crowther, of England, who visited the Soviet Union on seven different occasions and spent most of the winter of 1934-35 as guest of several scientific bodies, including many of the major institutes concerned with physics and chemistry. His book[2] gives a great deal of detail about the specific research problems in which many individual scientists were engaged in at the time of his long visit.

2. Eric Ashby, who went to Russia in 1945 as an official scientific representative of the Australian government and who gives an objective account of a scientist's observations and impressions of the organization of scientific effort and education.

3. Mrs. Harding, an English zoologist, who accompanied an expedition of scientists and physicians on a specially conducted trip in 1951 to meet colleagues in Russia.

4. C. Thompson, General Electric Co. engineer, who supervised power installations in Russia on three separate occasions: 1928 29; 1932-33; and 1946.

Defectors who have come out of Russia have sometimes provided useful information. In the main though, these have been workers on lower levels who have been informed only about limited aspects of the work with which they have been connected. A major reason for such limited knowledge is the fact that the security-mindedness of the Russians causes them to compartment their classified research so that only a small number of people at the top are informed about the entire problem. All others are so restricted in their work that they become familiar with only one component of the final equipment. They may have general ideas from their part of the effort of the purposes of the over-all program, but they learn the details of only that part on which they are directly engaged.

III. ESSENTIAL FEATURES OF RUSSIAN SCIENCE

In view of the fact that the U. S. S. R. is approaching its scientific task by methods quite different from those used in any other country in the world, it appears desirable to attempt a description and analysis of the essential features underlying its approach.

Governmental Control

The first and most important aspect of Soviet scientific effort is the fact that it is completely under government control. The effects of this control will be discussed under three headings: planning, decentralization, and expansion.

Planning

State planning of the scientific effort includes not only its scope institutions, personnel, equipment, and finances—but also its content, i. e., the directions it will take, the problems it will work on, the materials it will use, and the goals it will attempt to achieve.

In this planning, the Soviet Academy of Sciences plays the prominent role. It is "not only an advisory and policymaking body on matters of learning, but also the most important operating agency for the huge amount of organized research" that is being conducted.[3] It has a voice in the planning of numerous university and industrial research laboratories operating outside its sphere; it even suggests that specific activities proposed for development be assigned to designated institutes outside the Academy. In establishing programs, the individual research workers presumably submit their own ideas and plans; these go up through channels to the research committees of the individual institutes and thence to the appropriate division of the Academy. The decisions that are then made set the patterns of effort for the succeeding year and are supposed to provide the necessary authority and financial support.

The technological program, i. e., the goals assigned to industry, agriculture and transport, is normally set by the recurring Five Year

[1] Information about the Leipzig fair is given in *U. S. News & World Report*, 24 September 1954, p. 148.

[2] J. G. Crowther, *Soviet Science*, E. P. Dutton & Co., 1936.

[3] I. S. Sokolnikoff, "Organized Research in the U. S. S. R." *Scientific Monthly*, March 1951, p. 165.

Plans and within this general framework on a year-to-year basis in every one of the individual industrial establishments.

The outstanding consideration bearing on the Soviet government's attitude towards its science and technology is the great deal of encouragement which there have been given. The proportion of the national wealth which is being devoted to scientific endeavour is probably more than has been given by any other country of the world in recent years, or indeed at any time. The driving force which provides a major criterion in the decisions made is always the practicality of the effort under consideration—of how much service to the state will the results be. These decisions, which must perforce include a comprehensive examination of the order of priority of all the major portions of the year's effort, are also made to fit into a long-range program which is very broad and farsighted. As an example, it was realized, in Lenin's originally announced "Plan of Scientific and Technical Work," promulgated in 1918, that electric power would have to be expanded tremendously in order to cope with the ever-increasing demands that would be made on power sources. In keeping with this realization, a far-reaching program of large-scale power projects was given a high priority and pushed to such an extent that electrical output increased 25 fold between 1920 and 1940. And then, despite the war, the 1940 figure was multiplied by almost 2½ by 1952.[7] This was a big step in the transformation of the U. S. S. R. from an agrarian into an industrial country, a step sufficiently great to warrant its being highlighted by Stalin in a speech on 9 February 1946 to the voters of the Stalin Electoral District in the city of Moscow.[8] He referred to it as the accomplishment of a gigantic task in an incredibly short period.

Decentralization

The long-range plan of electric power development included an aspect that points up the controlled decentralization of Soviet science. A major purpose of this decentralization is the elimination of excessive dependence on any one area and the consequent enhancing of the national security. It has the additional advantage of establishing industry near the sources of its raw materials, thus reducing the strain on the entirely inadequate transportation system. The result of this planned decentralization is the development of new hubs of scientific activity; in the Far East, in Vladivostok; in the Urals, in Sverdlovsk; in Georgia, in Tbilisi; in Armenia, in Erevan; in Azerbaijan, in Baku; in Kazakh, in Alma-Ata. In these areas, new industries have been established, new sources of raw materials developed, new fuel and power facilities made available.[9] The larger factories have been furnished research facilities. Moreover, large new research institutes have been set up in such places as Dniepropetrovsk, Sverdlovsk, Novosibirsk, and Tashkent.[10]

Expansion

A third aspect of Soviet science is the great increase that has been sponsored in numbers of universities, colleges and students.[11] The Soviet Union has deliberately set out to take the world lead in the scientific and engineering fields. Through a constant program of popularization and publicity, science is kept very much in the public eye. Many types of inducements are offered to attract the better qualified students into these fields of effort and the cream of the educational system is skimmed for this purpose. Qualifying students are exempt from military service until they graduate. The social prestige of the scientist is a powerful attraction. Scientists are well paid—ten to twelve times as much as an average worker,—they are provided with better housing facilities, they are given special consideration for their families, rest homes are provided for vacation activity, bonuses and prizes are given for important contributions. In short, the field of scientific activity is made very attractive.

The enormous expansion of the institutions of higher education in the Soviet Union may be regarded as a measure of the energy and resources devoted to the preparation of technical and scientific personnel. From all indications, the entire educational power of the Soviet state appears to be committed to the goal of overtaking and surpassing the U. S. in the scientific and engineering fields. The number of graduates per year in science in the U. S. S. R. is growing very rapidly. At the present time, it is almost twice the corresponding number in the U. S.

The program for training top-level scientists and technologists to carry out research and direction of industry is accompanied by a similar program for training a second echelon of subprofessional technicians. This corresponds in a general sort of way to our vocational schools and junior colleges. It is relatively new in concept and seems to have been introduced by the Soviets to cope with deficiencies that had been brought to light in the educational system. The schools established

[7] A. V. Winter, *Soviet Electric Power Development*, Moscow 1952, p. 38.

[8] A. V. Winter, *op. cit.*, p. 35.

[9] B. G. Holzman, *An Appraisal of Soviet Technological Capabilities*, Individual Study, NWC, 1st Semester, 1951–52, pp. 7–9.

[10] J. G. Crowther, *op. cit.*, p. 22.

[11] Benjamin Fine, "Moscow is Overtaking U. S. in Training of Technicians," *N. Y. Times*, 7 November 1954, p. 1.

for this purpose are associated with existing enterprises, such as factories, which provide the teaching staffs.[12]

Of course, quantity alone is an inadequate criterion. What about quality? All the evidence we have about curricula, standards of training, performance of students after graduation, and about the character and difficulty of published research work appear to indicate that the Soviet scientists are on a par with our own. If we grant that a like proportion of their graduates and ours develop into top-level calibre then it must be concluded that if they are training twice as many scientists and technologists they must be developing approximately twice as many first-rate ones.

An interesting point worthy of mention before we leave this topic is made by Dobzhansky on the risks that may accompany the granting of unduly great importance to science.

> "But the exalted position of science and scientists in U. S. S. R. is purchased at a high price. It carries serious risks and penalties. First of all, some of the more ambitious and unscrupulous types of persons who in the West would seek more remunerative and influential positions, in U. S. S. R. choose science for their careers. More important still, the very magnitude of the investment which the state is making in science, and the great influence which science may secure on the popular mind, render it inevitable that a government of the type which exists in U. S. S. R. will tightly control science and will seek to exploit it for political propaganda purposes"[13]

Effect of Communist Ideology on Science

We come now to the consideration of a second feature: the Communist ideology and its effect on the scientific effort. This is a subject that has been given a great deal of attention over many years and about which some sweeping statements have been made. The general tone of most of these statements is to the effect that Soviet science is due to collapse, that the regimentation of Soviet scientific effort will cause it to fall flat on its face. The immediate cause of these remarks and of a great deal that was written on the subject was the now famed Lysenko controversy. To put it very briefly, Lysenko was a charlatan who succeeded through the use of politics in getting control of the field of genetics. With this control, he accomplished the deposition of geneticists. A few of them, including the brother of the President of the Academy of Sciences, disappeared from the Soviet scene and have not been heard of since.

The effect of this occurrence on the West was striking indeed. It gave rise to statements by some of the world's leading scientists that here was clear indication that science could not flourish in a regimented society. Professor Sirkle, of the University of Pennsylvania, who wrote a historical account of what had happened—insofar as it could be pieced together from such information as he had been able to get—entitled his book *Death of a Science in Russia*. Vannevar Bush in his book *Modern Arms and Free Men* said:[14]

> "Dictatorship can tolerate no real independence of thought and expression . . . No true fundamental science can flourish long under such a system, no matter what the individual genius may be . . . Science will eventually become a collection of superstitions and folklore. Men of genius will languish and succumb to discouragement . . . The system with which we contend cannot . . . even apply science to war in the forms it will take in the future, without mistakes and waste and delay."

Julian Huxley wrote a detailed examination of the Lysenko controversy in which he stated that:[15]

> "Nazi Germany paid for its attacks on scientific work. The U. S. S. R. will doubtless in due time pay an equally heavy price."

These points of view are still being expressed by some who continue to assert that the Soviet system contains within itself the seeds of its own destruction. And they point to similar detrimental effects of ideology on philology, economics, and statistics. But events of the last five years have raised some doubts. For example, the success of the Soviets in the production of nuclear bombs, of both the fission and the fusion types, in unbelievably short periods has confounded the predictions that it would be many years before the Soviets could hope to have atom bombs, if ever. We shall demonstrate in Section IV that the Soviets are making considerable progress in both the pure and applied fields of science. Vannevar Bush now says:[14]

> "We have now had some pretty convincing demonstrations of the success of Russian applied science. It's true, Russian weakness lies in the rigidity of its political system, but its application of science is evidently able to accomplish much."

Note also that the type of action which resulted in the Lysenko affair is definitely not irreversible. Indeed, Lysenko is on the way to being discredited.[16] Khrushchev, in February 1954, ridiculed a "so-called scientist" named Dmitriyev, whom he explicitly identified as a protégé of Lysenko. A few days later, Pravda printed a letter which referred to Lysenko's use of ideological arguments as a "mockery of Soviet science." Other critical statements about him have recently gone unchallenged. These developments may merely mean that Lysenko's ideas are not producing results and that he may have to make way for someone who can do better.

[12] Clifton Daniel, "Vocation Schools Opening in Soviet," *N. Y. Times*, 22 September 1954, p. 31.

[13] Dobzhansky, *op. cit.*, p. 40.

[14] "Red Science," *Newsweek*, March 1, 1954, p. 46.

[15] J. Huxley, *Soviet Genetics and World Science*, London, 1949, p. 196.

[16] "Lysenko Criticism Gains Volume," *Soviet Affairs*, OIR Report No. 4800.64, May 1954, pp. 13–15.

Without attempting to interpret such developments it remains true that we are really very poorly informed about just what effect Soviet ideology has on its scientific effort. Is it conceivable that the Soviets are actually succeeding in evolving a kind of existence which can simultaneously regiment politics and have little effect on science? Is it not true that the effects of ideology are felt only in limited areas of the entire scientific field? And is it not clear that where the concern is with obviously demonstrable applications of science (e. g., to military affairs), ideology plays a secondary role? Our present information furnishes no satisfactory answers to these questions.

Inculcation of Determined Attitude.

It is proposed now to discuss one further feature of the Soviet situation, *viz* the apparent existence of a spirit of determination and drive which spurs the people on to unusual achievements. Not much is known of the method by which this attitude is implanted but it certainly seems clear that when the Russians set themselves a goal they head for it with an amazing tenacity.

The recruiting of science students is a case in point. If a field of effort is considered to warrant a sufficiently high priority, the authorities go to great lengths to sponsor it.

Consider for a moment a field of activity entirely unrelated to science, the field of sports. For a long time, the Soviets did not compete at all in the Olympic Games. We don't know what their reasons were, and there does not seem to be any point in speculating about them. But once they decided that they would compete, they sent teams that really distinguished themselves; and it begins to appear probable that they may easily lead the field in 1956. Some aspects of their behavior in 1952 caused comments to the effect that the Soviets were approaching the Olympic Games with an attitude very different from that of all other countries. It was said, for example, that their entrants were not always sporting, and that they competed with a deadly sort of grimness. It was noted that the Soviets deliberately entered competitors in the less common events since they could thus have greater prospects of scoring points. The behavior of their team managers, who sometimes acted like MVD officials rather than sports coaches, was quite puzzling to their Free World opposite numbers. They argued about scores and about methods of tallying points.[17] They argued about procedure.

All this and much more provoked comment. Perhaps these were merely the excuses of Free World apologists who even questioned the amateur status of the Soviet entrants. In any event, the Soviet fanaticism did produce remarkable results.

[17] *Time*, 11 August 1952, p. 70.

A similar instance is found in the game of chess, which the Soviets have built up into a national pastime.[18] It is played very widely and great honor accrues to the players who distinguish themselves. The result of this attention to the game is that the present chess world is dominated by Soviet players. In a recent international tournament whose purpose was to pick a challenger for the world's championship (the present champion is a Russian, Botwinnik) and in which there were fourteen entrants, nine were Russians. Only two non-Russians ended up in the first half. All nine Russians had been sent at government expense to a special rest camp for almost a full month before leaving for the tournament. At the camp, they studied, attended lectures and were given special exercises to condition them physically. This last point may seem a humorous matter except for the fact that the scores during the tournament showed that the Russians performed significantly better against the non-Russians in the second half than they did in the first half. This can surely be attributed in large measure to the fact that they stood the strain of the competition better than those who had not been so well conditioned physically.

Psychologists may adduce in explanation of all this that the Soviets have a tremendous inferiority complex and are forcing themselves unduly by way of compensation. Be that as it may, this same kind of determination seems to pervade other aspects of the Soviet effort and, in particular, much of the Soviet scientific effort. Properly stimulated, such a drive can produce unbelievable results, as we have seen in the matter of the A- and H-bombs. Of course, it has its drawbacks too. It may well be that one result of such an attitude is that in those cases when they go off in a wrong direction, they go miserably wrong, so that their errors are really big errors. There have, in fact, been some apparently big blunders that call for an explanation. The important question for the Soviets in such instances is how long it will take them to realize that they are going in a wrong direction, and how much damage they may have done by that time.

How can we evaluate such a feature of the Soviet? Especially when there may be a real question as to whether the Soviets really have, in any unique sense, a greater drive than is found among people devoted to a cause in any other country. Assuming that it does exist, a quantitative evaluation is hardly possible. From a qualitative standpoint, suffice it to observe that a country is surely favored if it can profit from the inculcation in its people of a driving force towards those goals which its leaders have indicated to be of value to the country.

[18] P. Romanovsky, "Chess in Russia," *Soviet News*, London, 1946.

IV. PRESENT STATUS OF SOVIET SCIENCE AND TECHNOLOGY

We come now to the point where we try to find out from the evidence available to us what is the present status of Soviet science and technology. The distinction between these two terms is difficult to make and is sometimes artificial. In a very general sense, technology means applied science as distinguished from pure science, particularly such applications to methods and techniques as are used in industrial engineering, and agriculture, to improve and increase production. A fact, a theory, and a material can pass very quickly from the field of science to the applied field—so quickly indeed that it has become a commonplace among scientists. Much depends, of course, on the amount of emphasis and support which is given to sponsoring the advance of the concepts which have been developed. A Manhattan Project can save many years in going from a laboratory demonstration of uranium fission to the successful construction of an atomic bomb.

Such government support in terms of funds, facilities, and personnel becomes all the more necessary the greater the scope of the over-all program. This is a fairly recent type of development in the history of science and represents what is probably the greatest change from scientific effort of the past. Just think how long it took to go from the earliest discoveries in electricity to the commercial applications of electric power. There is a classic story about Benjamin Franklin, who, after one of his lectures on electricity, was asked by a kindly old lady, of what good was electricity. He answered, "Madam, what good is a new born baby?" This particular child matured very slowly. Large scale support by government or industry of scientific effort is a modern means of achieving a greatly accelerated aging of newborn babies. And the Soviets, in effect, have made a monstrous Manhattan project of all science.

There is undoubtedly a tendency for sponsored scientific effort to overemphasize applications of new knowledge at the expense of basic research. This is more apt to apply in industrial, private effort than in government. In either field skillful direction and understanding are required to derive the greatest long-range benefit from a program of scientific effort. Such capability and understanding have been present in U. S. industrial and university circles and have been important factors in our scientific and technological advances. Since in the Soviet Union, the programming must stem entirely from governmental direction, there is imposed upon such centralized, governmental control an increased responsibility for effectiveness.

How well they are coping with this responsibility can be gauged to some extent by the material that follows on the present status of the Soviet effort.

Pure Science and Research

There is considerable evidence from the open literature to demonstrate that the Soviets are doing quite well in pure science and research.

> "From being an extremely backward country in science only a generation ago, Russia has become an extremely important one. In some sciences, . . . it is already producing as good work as any country in the world, in older disciplines, in which other countries had already a long start over it, it has not yet been able entirely to catch up. But, on any standard, its achievement is remarkable."[19]

Their published work in mathematics, physics, chemistry, astronomy, and meteorology is very good indeed. So long as the field of effort is one which has no possible connection with Communist ideology, the work being done seems comparable to that in the Free World, and it can probably be said that in these fields the Soviets have pretty well pulled even with us. An idea—albeit, somewhat out of date—of the range of their researches in physics, chemistry, and biology can be obtained from the excellent and detailed presentation by Crowther.[20]

Let us consider some specific instances:

An extensive project conducted by the Air Technical Intelligence Center surveyed the entire field of Slavic geophysics between 1945 and 1952.[21] The primary interest of the study was to determine what work was being done in the investigation of the physical laws of the atmosphere which affect the operation of air-weapons systems. Thus papers in the following fields were examined:

Terrestrial Electricity and Magnetism
General Atmospheric Properties
Meteorology
Upper Atmosphere
Night Sky and Aurora
Meteorities
Solar Physics
Cosmic Rays

Over 800 publications were examined, at least in abstract. The following conclusions are drawn from the ATIC reports:

> "Over-all Soviet activities in the selected fields of geophysics are comparable to those of the United States. Soviet geophysicists are more active and their work appears to be of more significance than many people concerned in the U. S. may have realized. This is based on the large number of Soviet geophysical facilities that exist, the variety, number, and apparent technical level of problems investigated, and the number and apparent quality of the research personnel.

[19] C. H. Waddington, *The Scientific Attitude*, Penguin Books, 1941, p. 76.

[20] J. G. Crowther, *op. cit.*

[21] ATIC, Initial Report on the Status of Selected Fields in Geophysics in Foreign Countries, Project No. 9974, 15 June 1954, (SECRET)

> "The importance of some of the Soviet geophysical investigations to air operations, as is the case with U. S. investigations, is not directly evident However, since most of the Soviet research is basic in nature, the U. S. S. R. may be in a good position to make future developments, as such geophysical developments are largely predicated on previous fundamental research."[22]

As a second example, consider a field of activity which has recently attracted considerable interest in the U. S. It includes such aspects as linkages, mechanisms, servomechanisms, control and computing circuitry, and allied fields. The name that has recently been coined for it in our own literature is Automation. The Soviets are especially prolific in this field and publish most of their unclassified papers in a journal with the title *Automatics and Telemechanics*, which will soon become available to the U. S A special study by the ATIC states that the extent of the Soviet literature in these fields suggests[23] "that Russian design of mechanisms is based on better theoretical grounds than accepted practice in either England or the United States." As an interesting sidelight on the applicability of these ideas there is a paper by a Soviet scientist named Levin which discusses an automatic factory. In this paper, the author foresees the extension of automatic computing techniques to industrial processes.

Additional examples of capacity in other fields can be adduced. As a general statement, it can be said that the published material indicates that the Russians are clearly holding their own in pure research and are making important independent contributions. There are many who grant that this is so but who still insist that pure science cannot flourish in a regimented society, that such a society contains within it the seeds of its own destruction. Only time will demonstrate whether they are right. For our purposes though, it should be noted that those fields which are "out-of-favor" are directions of effort furthest removed from military applications and therefore have the least effect on the Soviet capability to wage war.

Technology

In technology, the general picture is not as clear as in pure science. The evidence, which is available to us in considerable quantity, leads to conflicting and contradictory implications with regard to Soviet capacity. In discussing such evidence, we shall list first indications of efficiency and competence, followed by indications of inefficiency and lack of competence

Evidences of Competence

Let us first examine some general indications of demonstrated competence.

[22] *Ibid.*, p. xii.

[23] *Soviet Capabilities in the Field of Computation Machinery*, Air Technical Intelligence Study, No 102-EL-6/52-34, 31 January 1952, p. iii (SECRET)

A basic requirement for an efficient technology is availability of plant capacity and raw materials. Although the Soviets are probably endowed with resources comparable in many senses to those of the U. S., they have nonetheless always been far behind the U. S. in their development and exploitation, but the extent of this handicap has been very considerably reduced in recent years.

Consider some key figures from Malenkov's report delivered 5 October 1952 at the 19th Communist Party Congress.[24] These are placed alongside U. S. data for comparison. (The figures are in millions of metric tons, except for electric power which is in billions of kilowatt hours.)

TABLE I

	U. S. S. R.			U. S.
	1952	Percentage Gain over 1940	Goal 1955	1951
Pig Iron	25	70	34	64
Steel	35	90	44.7	95.5
Coal	300	80	377	523
Oil	47	50	70*	307
Electricity	117	140	162	482

* (almost)

Granting that the Soviet Union has a long way to go before she can rival the U. S., it must be admitted that her gains are impressive. Further, it should be noted that Hitler challenged the world with only 22.7 million tons of steel production (1938). Beria, Bulganin and many other Congress speakers referred in this Congress to the Soviet Union's ability to convert rapidly to a war economy. In other basic materials, aluminum, copper, rubber and chemicals, similar impressive gains have been made.

The smaller quantities of basic materials at their disposal force Soviet engineers to conserve and make more effective use of their limited allocations. This they do very competently. Thus, conservation of materials is often revealed in their product design without

[24] *The Documentary Record* of the 19th Communist Party Congress and the Reorganization after Stalin's Death—from the translations of the *Current Digest of the Soviet Press*, Edited by Leo Gruliow, 1953, p. V, (Introduction).

significant effect on the resulting equipment.[25] When special alloys require critical materials, these are used sparingly. We know that the Soviets are familiar with most of the special alloys that we use, but it can be demonstrated that they use them much more sparingly when critical materials are involved. Voznesensky makes a virtue of this necessity.[26]

In this same connection, their designs are generally simpler and less versatile than ours, thus making the equipment easier to produce, operate, and maintain. The requirements for spare parts appear to be reduced below the levels that our corresponding equipment would normally require. On those occasions when it has been possible to examine the same type of item produced at different times, indications have been noted of definite improvement in technological competence.

The accusations sometimes expressed that the Soviets are mere copiers are entirely unfounded.[26] Even in those instances where they are known to have copied foreign equipment, the copying has been cleverly done, with enough aspects of redesign to show improvements in strength, performance, ease of production and cost of assembly. Althrough the general procedure has been to downgrade the quality of individual materials whenever feasible, there are instances known in which they have substituted higher grade materials than those used in the original equipment.

They have effectively mastered the general principJes of mass production, for they have risen in the field of industrial production from fifth place in the world to second, in one generation.[27] Cressey indicates that if the industrial index for 1913 is set at 100, that for 1938 is 908.8.[28] Even if we allow for some error in these figures, we have indication of improvement of a very high order of magnitude.

Let us now consider some specific examples in detail:

Russian communications equipment is relatively effective. Those items we have captured and studied seem to serve their purpose well. Note the following evaluation of a captured airborne transmitter:

> "The equipment is manufactured with all indications of high production run. Components are well arranged for accessibility of soldering and easy assembly. The frame of the transmitter is so designed that it can be placed in any position, i.e., top, bottom, side, etc., on the assembly line thus eliminating the necessity for a special fixture which normally would be used to carry the equipment along the line.
>
> "The set designers succeeded in achieving fair performance as simply as would be possible for a transmitter of this type.
>
> "Circuitry is basic, and there are no exceptionally good or poor design features in the set.
>
> "Good stability which ordinarily is not attributed to a modulated oscillator-variable frequency transmitter, was achieved by careful design and selection of components.
>
> "Because of the design simplicity, the equipment would be easy to produce, operate and maintain, and would require a smaller stock of spares than U. S. World War II equipment used for a similar purpose."[29]

A further instance of their effectiveness in communications techniques bears on their design and use of radio transmitters for jamming purposes. Apparently the broadcasts put out by VOA must be considered by the Russians to constitute a real threat, since they devote a considerable effort to jamming them. The Russians' jammers appear to have no other function: it is estimated that the jamming network employs roughly 10,000 scarce technicians and costs approximately 5 times more to run than the total cost of U. S. broadcasts to the orbit.[30] The point of interest from the technological view is that although U. S. stations often change their frequencies to get away from the jamming signal, the Soviets get on to the new frequency and retune their transmitters with a speed indicative of excellent equipment and excellent operation.

The Communists have also been expending considerable money and energy in broadcasts as a propaganda instrument.[31] Many broadcasts are clandestine and so well handled as to appear to the listener to be of local origin.

In the field of construction engineering, the Soviets have undertaken gigantic projects equal to anything found anywhere else in the world. This calls for large scale equipment which they have designed and produced. A caterpillar excavator designed and produced at Novo-Kramotorsk has a bucket with a capacity of 19 cu. yds. A drag line excavator with a similar capacity of 18 cu. yds. can cut into the ground at a distance of 50 yds. and dump a full load once a minute as far away as 130 yds. A crew of 15 engineers on such a machine can do the work of 7,000 or more men.[31] There are many other types of new machines scrapers, dump trucks, etc. On one major project, these and other machines will enable four billion cu. yds. of earth to be moved in 5 to 7 years—about 16 times the amount moved for the Panama Canal. In the construction of large buildings, the conspicu-

[25] Soviet Technological Skill Revealed by Materials Tests, *Soviet Affairs*, Aug. 1954, (OIR Report No. 4800.67) pp. 24-27 (SECRET)

[26] B. G. Holsman, *An Appraisal of Soviet Technological Capabilities*, Individual Study, NWC, 1st Semester, 1951-52, p. 8.

[27] Harry Schwartz, *op. cit.*, p. 622.

[28] G. G. Cressey, *The Basics of Soviet Strength*, McGraw Hill, 1945, p. 126.

[29] Analysis of Communications Equipment, ATIC Technical Report No. TR-EL-44, 6 December 1951, p. VI, (SECRET).

[30] "Soviet Bloc Improves Foreign Radio Net," *Soviet Affairs*, Dec. 1953, pp. 28 ff. (SECRET).

[31] S. M. Manton, *The Soviet Union Today—A Scientist's Impressions*, London, 1952, p. 87.

ous features are the giant crane and the simplicity of scaffolding.[32] Bricks are sent up to the bricklayers on conveyor belts or lifts from ground level.

Many more instances can be cited to indicate a highly efficient, favorable state of Soviet technology. It would appear probable that they can produce anything we can, provided they assign it a high enough priority. The rate of progress they have made during the five or six years immediately following the war has been phenomenal. Extrapolating with this rate over a long period, we can—and sometimes have[33]—come up with predictions that are frightening. But such a process of extrapolation is inadmissible. Apart from the point that high percentage increases are more easily accomplished on a smaller base, these rates of improvement include such special factors as the receipt by Russia of a great deal of U. S. equipment during the war, the acquisition of a large number of German scientists and technicians and the removal to the Soviet Union of entire industrial plants from occupied countries.

Besides, there is quite a case to be made for the view that Soviets are far from being supermen, and not anywhere near as good as the preceding evidence would lead us to believe

Evidences of Lack of Competence

There have been numerous indications of Soviet error, lack of efficiency, inability to meet planned goals, mistakes in allocations and in programming of effort, failure to achieve worker cooperation, unsatisfactory end products, etc. Despite the strict censorship imposed, despite the controlled handling of the dissemination of information, despite the constant propaganda efforts always to paint in bright colors even when the pigments were tarnished, information has regularly got out proving that there are lots of problems.

Thus, there has been repeated acknowledgement by the Soviet leaders of acute housing shortages,[34] this despite the fact that inadequate housing has been one of the most consistently dark aspects of the Soviet standard of living. Various estimates available for several different periods since the Revolution indicate that the average per capita housing space has been of the order of 4 to 6 square meters. The larger of these figures represents the space occupied by a square 7 to 8 feet on a side. The estimate for 1950 is somewhat under that for the mid 1920's when it was very poor. At that time the typical housing available for a small or medium sized family in a Soviet city was only one room, in an apartment containing three to six families, all sharing the kitchen and bathroom, if any.[35] According to a recent article in *Voprosy Ekonomiki*, the 1954 housing construction goal is 37.8 million square meters—9.8 million more than in 1953. The figgures given for actual construction in 1951, 1952, and 1953 are 27,27,28. It appears most unlikely that Soviet construction industry will be able to achieve the expressed goal. Scattered data indicate that even the foremost Soviet building enterprises are lagging behind plan. And suppose the goal could be met, it would represent a per capita increase of approximately 2 square feet for the entire year. Compare this with U. S. figures. We have been building over a million homes a year. A conservative estimate would allot 1,500 square feet on an average to each home, thus making a per capita increase of almost 10 square feet—an actual accomplishment five times as great as the expressed Russian goal, despite the fact that our requirement is nowhere near theirs.

A continuing series of Soviet press articles during recent months indicates that the growth of the Soviet coal industry is being hindered by technological difficulties, essentially a need for a radical change in mining technology.[36] Although coal output in gross tonnage terms has been increasing steadily since the end of World War II, and the industry has met or exceeded its production targets every year except one since 1947, the rate of progress does not appear to satisfy Soviet authorities.

In the peace terms of 1944, the Soviets acquired from Finland about seventy industrial concerns. They imported Soviet staffs to manage these going concerns and found, with the passage of time, that competitive conditions were too rough for them. Well over half were sold during the past year—all to Finnish buyers.[37] A Finnish official who has been keeping a close eye on these developments says there's hardly any doubt now that the Soviets are out to sell them all. Their management staffs are just not up to the tasks that have been assigned them.

The production goals set in the 5-year plans are seldom achieved. Perhaps it is because they are deliberately exaggerated as a mechanism for spurring on endeavour, but if so then it is not easy to explain the constant carping and criticism that gets into official pronouncements.

[32] *Ibid.*, p. 22, fig. 6.

[33] Soviet Air Forces, *Air Technical and Scientific Capabilities*, Air Intelligence Study, AIS 2-28, 1 April 1953, Def t, USAF and ONI, p. viii, (SECRET).

[34] "U. S. S. R. Steps up Efforts to Improve Housing," *Soviet Affairs*, November 1954, pp. 16, 17

[35] Harry Schwartz, *op. cit.*, p. 453 ff.

[36] "Technological Problems Plague Soviet Coal Industry," *Soviet Affairs*, November 1954, pp. 17–19.

[37] M. Gordon, "Soviet Plants in Finland Find the Capitalist Competition Too Tough," *Wall Street Journal*, 2 December 1954, p. 1.

> "As late as September 11, 1950, *Pravda* found it necessary to print a long article complaining about the frequently low productivity in Soviet plants."[38]

Other manifestations of inadequate productivity are seen in the Soviet Union's failure to meet commitments in foreign trade. For example, in September 1954, reports from Argentina indicated disillusionment in her attempts to do business with the Soviets.[39] A trade agreement with the Soviet Union was supposed to do big things for Argentina and was to serve as the basis for expanded Soviet trade in Latin America, but it is not working out that way. Argentina started shipping exports to the Soviet Union shortly after the agreement took effect. The Soviet deliveries, if made at all, are falling far short of promises. In particular, the Soviets are failing to deliver promised capital equipment—farm machinery, generators, transmission equipment, and oil-field equipment.

Finally we need but mention, without going into detail, such considerations as the effects of regimentation and compartmentation, the disadvantages of bureaucracy, the omnipresent MVD and its detrimental effects on freedom of thought and inquiry, the low living standard of workers, the serious inefficiencies of Soviet transport and many other deficiencies which must have detrimental effects on their technology.

When we try to weigh in the technological balance the evidences of efficiency and capability in the one pan against those of inefficiency and lack of accomplishment in the other, we find that the pointer of the scale wobbles so violently—now tipped one way, now the other—that it is not possible in our present state of intelligence to arrive at a satisfactory reading. This naturally complicates our problem of prognostication.

FUTURE PROSPECTS

What then shall we say about the future of Soviet science and technology? It is a difficult subject in which to make predictions. Some highly competent people in this country have made very wrong guesses. Witness the testimony in 1945 of Vannevar Bush and General Groves before a Senate Committee that was studying the possibility of the Soviets' producing nuclear weapons. Other instances can be cited of relatively recent opinions about Soviet capability which have already been shown to be far wide of the mark.[40]

We cannot doubt in any event that the Soviet Union is a ranking power in science and technology. She is advancing at the present time at a rate faster than that of the U. S. and if these relative rates remain unchanged for any lengthy period, then it follows that with time the Soviet Union could pull even with and then surpass the U. S.

In this matter of comparative rates, the point should be kept in mind that much of the work done in the Free World is readily available to and being utilized by the Soviet Union. An idea of the vigor with which such information is sought and collected by Soviet representatives in the U. S. can be gained from an article in the *ONI Review for Mid-summer 1954*, entitled "Soviet Intelligence Collection in the U. S."[41] A much smaller percentage of Soviet results is getting to the Free World and our scientists are not giving that smaller amount as much attention as it may deserve. This is an additional factor making for long-term advantage to the Soviet Union.

As the Soviet technological situation improves and the production of consumer goods is expanded, the general living standard of the Soviets will continue to rise. We might hopefully look forward to a time when the Soviet situation is sufficiently improved to change their outlook on world affairs and cause them to live in greater harmony and cooperation with the rest of the world. But this is clearly a kind of wishful thinking and not justified on the basis of anything we have seen since the end of the war.

Assuming an indefinitely continuing cold war, there will be continued emphasis on research into military weapons, both offensive and defensive types. From all indications, the Soviets are devoting a relatively greater percentage of their budget and of their national capability to these matters than we are.

Now science is not static. Advances are being made continuously. Despite the fact that nuclear weapons represent a tremendous advance over anything that had preceded them, it is an error to think of them in their present form as representing any sort of ultimate accomplishment. They can be improved on and no doubt will. Of the total energy available in the uranium of an atom bomb, only one tenth of one percent is actually utilized in the explosion.[42] There is considerable room for improvement in the power of nuclear weapons.

Improvements can also be anticipated in the methods of delivery of bombs. After all, the intercontinental guided missile is already in sight. Such developments then as increased size and improved delivery are readily conceivable. In the light of the present stalemate, I do not believe that nuclear weapons will be used by either side in the forms

[38] Harry Schwartz, *op. cit.*, p. 652.

[39] *U. S. News & World Report*, 24 September 1954, p. 85.

[40] Harry L. Hillyard, *Soviet Science and Technology: Present Levels and Future Prospects*, Individual Study, NWC, November 1953, (SECRET), pp. 2-6.

[41] "Soviet Intelligence Collection in the U. S.," *ONI Review*, Supplement, Mid-Summer 1954, pp. 7-11. (SECRET).

[42] Samuel Glasstone, *Sourcebook on Atomic Energy*, van Nostrand, 1950, p. 418.

now known to us or even in the forms to be anticipated in the near future.

What should really worry us is not the weapon or the method of delivery that we can conceive. What we ought to be concerned about is the next step that we cannot now forecast. Just suppose that the basic development in science within the next ten or twenty years is a new weapon as decisively superior to the A- and H-bombs as they were to their predecessors.

That such an idea is far from fantastic can be easily demonstrated. In June 1937, the Science Committee of the National Resources Committee submitted to the President a report entitled *Technological Trends and National Policy Including the Social Implications of New Inventions*. Contributed to by many eminent scientists, it was intended to consider aspects of national policy which had to be kept in mind as a result of new inventions which might develop within the next ten to twenty-five years. It does not even mention atomic energy. The date warrants repeating—June 1937, and it was not considered that atomic energy would be a matter of concern in the succeeding 10 to 25 years!

Suppose then that the next basic military development is a new military weapon decisively superior to nuclear bombs or an effective defense against nuclear weapons. Suppose the Soviets develop it first and push it to an advanced stage or produce it in quantity even before we become aware of it. What could we do if we were suddenly threatened with such a situation. That to my mind, is the real danger that confronts us, and which we must aim to prevent by every strenuous means in our power. We must not lose the scientific race against the Soviets for to do so means losing the war– be it cold or hot. We feel certain we have the ability to win; we are convinced we have the better system; if we make proper use of our ability and our system we will win.

BIBLIOGRAPHY

Individual Studies and Lectures

1. Hillyard, Harry L., *Soviet Science and Technology, Present Levels and Future Prospects*, Individual Study, NWC, November 1953.
   This study gives the Soviets a high capability rating and concludes with the expression of a possibility that the Soviets could surprise us with new and perhaps decisive weapons.
2. Holzman, B. G., *An Appraisal of Soviet Technological Capabilities*, Individual Study, NWC, First Semester, 1951–52.
   This appraisal points up the predominant role that nuclear capability plays in a comparison of U. S. and Soviet technological strengths.
3. Patterson, Charles G., *Soviet Science and National Power*, Individual Study, NWC, 1952–53 (RESTRICTED).

Contains an interesting discussion of the possible effects of thought control on Russian science and a provocative list of questions concerning Soviet science and technology.

4. Samuels, Andrew, Jr., *An Appraisal of Soviet Technological Capabilities*, Individual Study, NWC, October 1950.
   An objective appraisal largely concerned with the applications of Soviet technology to military capability.
5. Thompson, C., *Russian Technology*, NWC Lecture, 22 October 1948.
   An account of the supervision of power installations in Russia, both before and after the war.

Books

1. Air Intelligence Study, Soviet Air Forces—Air Technical and Scientific Capabilities, AIS 2-23, AF 656607, 1 April 1953. (SECRET).
   General summary of the current state of knowledge of Soviet air capability. Covers aircraft, armament, guided missiles, electronics, aeromedical and basic sciences.
2. Air Technical Intelligence Center, *Analysis of Communications Equipment*, ATIC Technical Report, NOTR–EL–44, 6 December 1951. (SECRET).
3. Air Technical Intelligence Center, *Initial Report on the Status of Selected Fields in Geophysics in Foreign Countries*, Project No. 9974, 15 June 1954. (SECRET).
4. Air Technical Intelligence Center, *Soviet Capabilities in the Field of Computation Machinery*, ATIC Study No. 102–EL–6/52–34, 31 January 1952. (SECRET).
5. Air University, Human Resources Research Institute, *The Soviet Doctor—A Case Study of the Professional in Soviet Society*, December 1952.
   An examination of the social role of medicine in Soviet society.
6. American Association for the Advancement of Science, *Soviet Science*, (A symposium of the AAAS in Philadelphia), 27 December 1951.
   This book contains a great deal of interesting information about various fields of activity in Soviet Science, and some prognostications by leading scientists.
7. Ashby, Eric, *Scientist in Russia*, Penguin Books, 1947.
   The author spent a year (1945) in Russia as an official scientific representative of the Australian government, and gives an interesting report of the scientific effort of the U. S. S. R. chiefly from the point of view of education and research.
8. Counts, George S. and Lodge, Nucia, *The Country of the Blind—The Soviet System of Mind Control*, Houghton Mifflin Co., Cambridge, Mass., 1949.
   A study of the manner in which the Soviets are using learning and culture as weapons in their ideological program. Specific attention given to literature, drama, music, science, education. A course of action for America is outlined.
9. Cressey, George B. *The Basis of Soviet Strength*, McGraw Hill Co., 1945.
   An interesting study of the Soviet Union, its history and geography, its people, resources and extent of industrialization. Some guesses with regard to the future.
10. Crowther, J. G., *Soviet Science*, London, 1936.
   The author visited the Soviet Union on seven different occasions during the seven years preceding 1936. The main material for the book was collected on a lengthy visit in the winter of 1934–35 when the author was the guest of several scientific institutes. He describes in considerable detail the research problems under study at all of these institutes and to some extent the conditions under which the research was performed.

11. Huxley, Julian, *Soviet Genetics and World Science*, London, 1949.
A detailed examination of the Lysenko controversy by one of the world's leading biologists.

12. Keller, B. A., *The Soviet Scientist*, Moscow, 1939.
A eulogy of Soviet Science as compared with science under the Czars and in "capitalist" countries. The tone is clearly one of bias and somewhat boastful.

13. Littlepage, John D., *In Search of Soviet Gold*, Harcourt, Brace & Co, 1938.
A story of ten years' work in Soviet Russia in the service of the Soviet gold trust. The period covered, 1927 to 1937, was an important formative period in the development of Russia's mining industry.

14. Manton, S. M., (Mrs. Harding) *The Soviet Union Today—A Scientist's Impressions*, London, 1952.
Mrs. Harding is a zoologist in the University of London, who was invited to accompany an expedition of scientists and physicians to meet scientific colleagues in Russia. Her book is biased but does contain a good deal of factual information.

15. National Resources Committee, *Technological Trends and National Policy Including the Social Implications of New Inventions*, Washington, 1937.
With the hindsight of the 1950's this document makes fascinating reading about predictions regarding future scientific endeavour.

16. Romanovsky, P. "Chess in Russia," *Soviet News*, London, 1946.
An account of how chess has been made a national pastime, together with indications of how it is encouraged and sponsored.

17. Schwartz, Harry, *Russia's Soviet Economy*, Prentice Hall, 1950.
A detailed study of all phases of Russia's economy. Chapters on industry and production are most useful.

18. Timoshenko, V. F., *The Soviet Sugar Industry and its Postwar Restoration*, Stanford University, 1951.
An interesting study of the beet-sugar industry in Russia.

19. Vavilov, S. I., "The Progress of Soviet Science," *Soviet News*, 1951.
Translation of an article taken from the book by Academician Vavilov entitled "The Science of the Stalin Epoch," published by the Academy of Sciences in 1950.

20. Waddington, C. H., *The Scientific Attitude*, Penguin Books, 1941.
A general discussion of the role of science and the habit of scientific thought in human society. Includes a brief chapter entitled "Is Communism Science?"

Articles

1. Ashby, Eric, "Soviet Science Is a Challenge to Us," *N. Y. Times Magazine*, 18 April 1954, p 13

2. Fine, Benjamin, "Moscow is Overtaking U S. Training of Technicians," *N. Y. Times*, 7 November 1954, p. 1.

3. "Red Science . . for the Military, Good; for the People, Poor," *Newsweek*, 1 March 1954, pp. 46–50.

4. "Soviet Intelligence Collection in the United States," *ONI Review* Secret Supplement, Mid-summer, 1954, pp. 7–11.

5. 'Soviet Technological Skill Revealed by Materials Tests," *Soviet Affairs*, OIR, Report No. 4800.67, August 1954, (SECRET) pp. 24–27.

The Borders of Cryptology

(b)(3)-P.L.
86-36

BY [redacted]

~~Top Secret~~

A discussion of electronic warfare activities that are closely related to cryptology.

The cryptologic partnership in its present form has evolved from a long series of reorganizations. In the process. functions which were similar or interdependent, but separately organized and perhaps not well coordinated. were brought closer together. The togetherness was accomplished by organizational mergers and by improved liaison.

By current definition, we now have only COMINT and COMSEC activities within the borders of cryptology. On the COMSEC side, our cryptographic security and transmission security responsibilities extend to all types of electronic emission. On the COMINT side, however, a distinction is made between "communications" and "non-communications" signals. Only the former are within the province of COMINT.

ELINT activities remain outside the borders of cryptology. ELINT arrangements probably are better known to the cryptologist than the arrangements for any of the other bordering activities. In many respects, COMINT and ELINT functions are similar and interdependent; a closer organizational merger is being developed; the term "SIGINT" (which covers COMINT and ELINT) has been added to our jargon.

In this article, we shall consider other bordering activities which currently or potentially have an important effect on cryptology, and to which perhaps the cryptologist has not given much thought. Those activities are jamming and electronic deception in particular, and electronic warfare in general.

Although we may observe that certain electronic warfare activities and cryptology or SIGINT are similar and interdependent, we do not intend to raise here any questions of further reorganization. From our broad review of current relationships, however, we should recognize at least the potentialities for close liaison among the bordering activities.

The two major subdivisions of electronic warfare are electronic countermeasures (ECM). and electronic counter-countermeasures (ECCM). Jamming and electronic deception are examples of *active* ECM. Search. intercept, D/F, range estimation, and signal analysis, when conducted for *steerage* of active ECM, are examples of *passive* ECM. The steerage of a jamming operation, for instance, would include the transmission frequency and identifying characteristics of the signal to be jammed. The term ECCM covers anti-jamming or anti-deception measures.

(b) (3)-P.L. 86-36 [redacted]

[redacted]

In view of the possibilities of security compromises, interference, and self-deception, U.S. communications jamming and imitative deception operations are subject to USIB approval in advance. USIB has specified circumstances in which this advance approval has already been given. USIB has also prescribed the conditions for conducting an operation when time does not permit the obtaining of advance approval. NSA is required to arrange for military commanders to be advised of the status of approval for a given operation. In addition, NSA is required to arrange for the necessary SIGINT support. While SIGINT units would give, they would also receive. When SIGINT activities are performed outside the scope of NSA's authority, there would be an arrangement whereby the results would be furnished to SIGINT units designated by NSA.

[redacted]

While the cryptologist will be affected by ECM efforts of the U.S., he will also play an important role in those situations in which the U.S. observes or is the victim of foreign ECM. The COMSEC specialist participates in the development of anti-jamming measures. He develops authentication systems and other anti-deception measures. Interception and analysis of foreign ECM signals is a SIGINT task. The analysis of foreign imitations of U.S. signals, however, would concern the COMSEC specialists more than the SIGINT people. The latter would be concerned with technical studies of jamming signals and with techniques for seeing through manipulative deception.

Electronic warfare activities have little noticeable effect now upon cryptologic or SIGINT activities. The Soviet signals which jam the Voice of America have been subjected to thorough technical analyses by ELINT activities. Aside from the extensive Soviet jamming of the Voice of America and of similar broadcasts by the West, there is practically no evidence that active ECM operations are being conducted now by the Soviet Bloc or by the West. Active ECM operations by the U.S. are limited in view of the various risks mentioned above and the high-level controls which call for special authorizations. Similar controls have been established in the electronic warfare policy of NATO. In additon to the risks we have mentioned (e.g., the possible loss of SIGINT security, or the possible interference with SIGINT collection), there is the danger that increased

[redacted]

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

(b)(3)-P.L. 86-36 [redacted]

active ECM operations by the West now would stimulate greater use of active ECM by the Soviet Bloc.

Although current use of active ECM is limited, much effort must now be devoted to electronic warfare problems. We should not attempt to predict here the solutions to the problems, but we should mention some of the major issues which would affect cryptology.

The electronic warfare policy promulgated by the Joint Chiefs of Staff provides for the development of an effective ECM capability. Similar provisions are contained in the NATO electronic warfare policy.

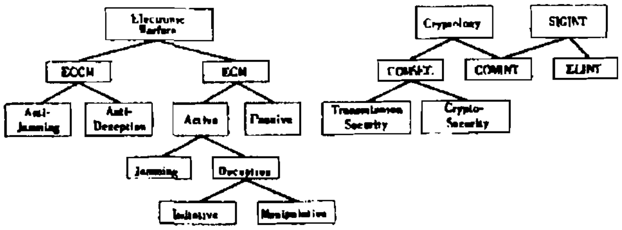
The development of an effective ECM capability implies the readiness of active and passive ECM specialists, suitably trained and equipped to handle operational tasks on short notice. Several NATO countries look to the U.S. for assistance in training and equipping units for active and passive ECM. It is difficult to provide for realistic training in passive ECM without revealing sensitive technical SIGINT information.

The problems of assisting in the development of an allied country's ECM capabilities are considerably more complex than those encountered in the development of U.S. capabilities. The complicating factors include the U.S. restrictions on COMINT, ELINT and COMSEC collaboration with foreign countries. The problems are also complicated by the several fundamental differences which are indicated in individual nations' views on COMINT-ELINT-COMSEC electronic warfare relationships. If our present restrictions were to be relaxed, the risks of compromise of course would increase, but we would be in a position to advise the recipients on security principles. If our restrictions were to be maintained, we might expect several NATO countries to exchange their sensitive technical information in arrangements which would exclude the U.S. In that event, the information might be handled under increased risks of compromise without the benefit of U.S. advice on security principles. Among the fundamental differences of views on COMINT-ELINT-COMSEC electronic warfare relationships, some NATO countries have expressed the view that passive ECM units should not only be trained and equipped, but also operational now; that they should contribute to an international exchange of electronic warfare intelligence.

While fundamental differences may exist in individual nations' views, there are also problems within the U.S. on the matter of determining details of COMINT-ELINT-COMSEC electronic warfare relationships. The exact borders of cryptology may often be questioned. Attempts have been made to draw the line according to raw materials or processes, but those attempts have not been completely successful. Having decided, for example, that COMINT and ELINT are distinctive, we can easily illustrate the distinction in terms of radio-telegrams and radar signals. We might have some difficulty, however, in determining whether a new type of signal from an earth satellite vehicle is in the province of COMINT or ELINT. As far as processes are concerned, we might attempt to place within the borders of cryptology the "specialized" processes in cryptomathematics, crypto-linguistics, etc., but on close examination some of the specialized processes are borderline. They resemble work done in non-cryptologic areas of government, industry, and educational institutions.

[redacted]

The bordering activities which we have considered are summarized below in chart form. The chart probably takes in all of the main subdivisions in the electronic warfare complex, but we are not absolutely certain that it does. We know, for example, that active ECM *includes* jamming and deception; if there are other types of active ECM, we do not know what they are.



In our comments here on existing relationships among bordering activities, we are criticizing and applauding as little as possible. But it must be apparent that these relationships are not perfect. Not all significant issues have been settled yet. Some which have been settled are still not easily understood. Some which may be understood do not seem entirely

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

logical. The imperfections cannot be traced to flaws in a master plan for the related activities; there is no such plan. The authorities who drew up national policy on COMINT, ELINT, and COMSEC were not the same as those who developed electronic warfare policy. The need for a master plan was not apparent when the separate policies were budding. Good progress has been made, especially during the past few years, by the several authorities concerned toward satisfactory settlement of individual issues. The progress is likely to continue by working on individual problems instead of attempting to solve them all at once by drawing up a master design now.

We have indicated the potentialities for close liaison among the bordering activities. The individual cryptologist may wonder what his own role will be. The liaison channels are still in an early stage of development. Relatively few cryptologists have been designated to conduct such liaison. As the number grows, the individual's duties will be apparent in technical instructions, terms of reference, appointments to panels, etc. The majority of cryptologists may never be designated to perform a liaison function, but they may nevertheless expect to be assigned some tasks which will support electronic warfare activities, or to be consulted by liaison people on some aspect of those activities.

A Program for Correcting Spelling Errors

BY [redacted]

Unclassified

(b)(3)-P.L. 86-36

A description of a program using a simple, heuristic procedure for associating "similar" spellings, which is able to correct misspelled words. Given only a vocabulary of properly spelled words, the computer can correct most (including unanticipated) misspellings without human assistance. Apart from practical applications, the process is interesting as an example of an unusual form of pattern recognition.

It is tempting to assume that English spelling is too irrational to be explained to a computer. If we limit ourselves to algorithms, perhaps this is true; yet if we give the machine an extensive vocabulary, it can be programmed to recognize as misspelled any word that is not in this list. Even this procedure will not detect all errors, for some misspellings are correct spellings of different words (e.g., *advice* can become *advise*). Since such errors can only be detected through context, I avoid this troublesome prospect by considering them as usage rather than spelling errors, and so outside the scope of my title.

Having discovered a word that is not in its vocabulary, what should the program do next? Obviously, it could maintain a dictionary which associates every misspelled word with its correctly spelled equivalent. But, this auxiliary dictionary is potentially several times longer than the already sizable vocabulary of correctly spelled words. Unless the basic vocabulary is extremely limited, maintenance of the auxiliary dictionary is impracticable.

Any hope of programming customary orthographic "rules" is destroyed at first glance; for, while a machine could easily put "'i' before 'e' except after 'c' . . .", it would have difficulty recognizing " . . . and when pronounced 'a' as in neighbor and weigh". Such coding difficulties, the numerous exceptions, and the lack of rules to cover many spelling errors make this approach unpromising.

If a spelling error is correctable without reference to the context in which it appears, then the misspelling must be sufficiently "close" to the correct spelling to permit unique association. Thus, if a machine is given a suitable criterion for computing the "similarity" of words, it can "correct" a spelling error by substituting the "most similar" correctly spelled word for the misspelling. In pattern recognition terms, a misspelled word is a pattern that is approximately equivalent to its correct version. Recognizing erroneous spellings requires devising some means of dividing all spellings into equivalence classes and giving the name of the class to each of its members.

(b)(3)-P.L. 86-36

How is "similarity" to be measured? One immediately thinks of ad hoc rules (e.g., if all other letters are the same, a word containing "ie" is very similar to a word containing "ei");[1] but programming them introduces the same difficulties that arise in programming orthographic "rules".

One approach to associating "similar" words is exemplified by the Soundex method, which files names according to a code based on their pronunciation. To form the code, the initial letter of the surname is followed by a 3-digit number which is constructed by ignoring vowels and assigning the same digit to similar sounding consonants in their order of occurrence.[2] The filing clerk can then select the proper individual from the section of the file specified by this code on the basis of given names or other identifying information.

Although widely and successfully used by human clerks, Soundex is not readily adaptable as a machine process for correcting spelling errors. To be sure, the code construction could easily be programmed, but the fact that it associates correct spellings of different words means that an additional distinguishing criterion is required. It seemed more efficient to search for a single "similarity" measurement which normally would uniquely associate a misspelling with its correct equivalent.

An abbreviation is a particular type of "misspelling" which retains enough "similarity" to the original word to permit unique association. Unique association implies that the abbreviation retains the meaningful "kernel" of the word. A spelling error, to be recognizable without using context, must also contain the meaningful "kernel". Thus, we are led to assume that two words are "similar" if their abbreviations are identical.

An r-letter abbreviation of an n-letter word can be produced by deleting those n−r letters which are least important in the identification of the word. The problem of producing an adequate abbreviation is, in application, that of deciding which letters in a word are the least important in determining its meaning. Information theorists assume that the information conveyed by a "message" is inversely proportional to its a priori probability of occurrence. One can apply this idea by eliminating the n−r letters in the order of their expected frequency; we tried this but found that even better results can be obtained by using the "frequency" of their occurrence as errors. An empirically constructed approximation of the latter function is given in Table I. The inadequacy of this technique is soon revealed by encounters with abbreviations such as "xpnn" for exponent. Clearly weight must also be given to the position of the letter in the word. The first letter is of greatest importance, and, all other things being equal, the last letter is second in importance, followed by the second letter, the next to last letter, etc. That is, if we reorder the letters in this fashion, the desirability of rejecting a letter in a given position is an increasing, monotonic function of the new position. An empirically constructed approximation of this function is given in Table II.

Table I
The Logarithm of the Desirability of Deleting a Letter as a Function of Its Name

Letter	Score	Letter	Score
A	5	N	3
B	1	O	4
C	5	P	3
D	0	Q	0
E	7	R	4
F	1	S	5
G	2	T	3
H	5	U	4
I	6	V	1
J	0	W	1
K	1	X	0
L	5	Y	2
M	1	Z	1

Table II
The Logarithm of the Desirability of Deleting a Letter as a Function of Its Position

Position	Score	Position	Score
1	0	9	5
2	1	10	5
3	2	11	6
4	3	12	6
5	4	13	6
6	4	14	6
7	5	15	6
8	5	16 up	7

By assuming that the name and position of a letter independently determine the desirability of rejecting it, one can form an r-letter abbreviation by deleting the n−r letters which have the largest product.[3] Although the assumption of independence is not strictly true, it is sufficiently accurate for our purposes. More refined results could be obtained by storing the larger table required for dependent variables.

Before it is asked to correct misspelled words, the machine must compute and store a short (we used 4 letters) abbreviation of each

[1] An extensive collection of such rules is given in: *Searching Aids for Alphabetic and Soundex Files.* Remington Rand Management Controls Division, New York. n.d.

[2] This statement is slightly oversimplified. For further details see: *Soundex.* ,Remington Rand, New York, n.d.

[3] To minimize time and storage requirements, 3-bit logarithms are added to compute the "product." The crudity of our estimates justifies no higher precision.

Example

A	B	S	O	R	B	E	N	T		A	B	S	O	R	B	A	N	T
5	1	5	4	4	1	7	3	3	Letter Score	5	1	5	4	4	1	5	3	3
0	2	4	5	5	5	4	3	1	Position Score	0	2	4	5	5	5	4	3	1
5	3	9	9	9	6	11	6	4	Sum of Scores	5	3	9	9	9	6	9	6	4
		*	*	*		*	*		Delete			*	*	*		*	*	
					A	B	B	T	Abbreviation	A	B	B	T					

correctly spelled word in the vocabulary. These abbreviations are then associated with their complete spellings and sorted. The machine can now correct misspellings in any text which contains only those words in its vocabulary. Reading the words in order, it forms their abbreviations and selects all identical abbreviations of correctly spelled words. Normally this process gives a unique answer and the spelling associated with the abbreviation is then used for output (see example). When an abbreviation coincides with more than one vocabulary entry, the program compares longer abbreviations of this input word with longer abbreviations of the vocabulary entries it matched until a unique one has been selected. Of course, it is possible that a misspelling will be so extreme that its abbreviation will not appear in the vocabulary. When this happens the machine can do no more than indicate that this word was unidentifiable.

The association of common misspellings[4] with their correctly spelled equivalents is illustrated in Table III. The program correctly identified 89 of the 117 misspelled words (3 required longer abbreviations) while incorrectly identifying only 2.[5] Before condemning the machine's performance, test yourself by covering the correctly spelled column and see how well you compare. Unless you are an exceptional speller, it will be an illuminating - and humbling - experience.

The two types of deficiency are easily detectable and correctable. A word that has been incorrectly identified by the program is virtually always conspicuous because it does not fit the context and a word not identified at all is made apparent by the blank space left in the output. These errors arise either because the word was not in the original vocabulary or because the misspelling was so extreme that it gave rise to a different abbreviation. The first type of error can be corrected by simply adding the new word to the vocabulary at the next updating run. The second type requires a certain amount of "cheating". A special vocabulary updating is used in which the correct spelling of this word and the abbreviation of the particular misspelling are placed in association in the vocabulary. Although inelegant, this procedure is quite efficient in allowing for peculiar exceptions and words that are too short to permit deleting all incorrect letters while maintaining the selected length of abbreviation.

Since this heuristic process was specifically designed for the type of spelling errors normally made by people, it is considerably less effective in correcting other types of errors. It would, for example, have little utility in correcting the output of a malfunctioning machine; fortunately, however, we have other means of dealing with these. Similarly, it is not difficult to construct "misspellings" that the process will fail to correct, but it is surprisingly difficult to select such errors from the writings of people.

The author desires to acknowledge the valuable assistance of Mr. R. W. Tobin, who prepared the programs used to test these ideas.

Table III

Examples of Associating Incorrect Spellings With their Correct Equivalents by "Abbreviation"

Correct Spelling	Abbreviations	Incorrect Spelling
ABSORBENT	ABBT = ABBT	ABSORBANT
ABSORPTION	ABON ABBN	ABSORBTION
ACCOMMODATE	AMDT = AMDT	ACCOMODATE
ACQUIESCE	ACQC AQUS	AQUIESE
ANALYZE	ANYZ ANZE	ANALIZE
ANTARCTIC	ANTC = ANTC	ANTARTIC
ASININE	ASNN = ASNN	ASSININE
ASSISTANCE	ASTN = ASTN	ASSISTENCE
AUXILIARY	AUXY = AUXY	AUXILLARY
BANANA	BANA = BANA	BANANNA
BANKRUPTCY	BAKY = BAKY	BANKRUPCY
BRETHREN	BRTN = BRTN	BRETHEREN
BRITAIN	BRTN = BRTN	BRITIAN
BUOYANCY	BUYY BOYY	BOUYANCY
CATEGORY	CATY = CATY	CATAGOREY
CHAUFFEUR	CFFR = CFFR	CHAUFFUER
CHIMNEYS	CMYS CHMS	CHIMNIES
COLISEUM	COUM = COUM	COLOSIUM
COLOSSAL	COAL = COAL	COLLOSAL
COMMITMENT	COMT = COMT	COMMITTMENT
COMMITTEE	COMM = COMM	COMMITEE
CONCEDE	COND = COND	CONSEDE
CONSCIENTIOUS	CONS = CONS	CONSCIENTOUS
CONSENSUS	CONS = CONS	CONCENSUS
CONTROVERSY	COVY = COVY	CONTROVERCY
CORRUGATED	COGD = COGD	CORRIGATED
CYNICAL	CYNL SYNL	SYNICAL
DEUCE	DUCE = DUCE	DUECE
DEVELOP	DVOP = DVOP	DEVELLOPE
DIGNITARY	DGRY = DGRY	DIGNATARY
DISAPPOINT	DINT = DINT	DISAPOINT
DRASTICALLY	DRTY = DRTY	DRASTICLY
ECSTASY	ECTY = ECTY	ECSTACY
EMBARRASS	EMBS = EMBS	EMBARASS
EXAGGERATE	EXGT = EXGT	EXAGERATE
EXISTENCE	EXTN = EXTN	EXISTANCE
EXTENSION	EXTN = EXTN	EXTENTION
FEBRUARY	FBRY = FBRY	FEBUARY

[4] From: Hutchinson, L. I. *Standard Handbook for Secretaries, Seventh Edition.* McGraw-Hill, New York. 1956. pp. 133-134. Reprinted by permission.

[5] Interferred became intercede and philipinoes became Philippines. Neither of these errors would have occurred if 5-letter abbreviations had been used.

(b)(3)-P.L. 86-36

[redacted]

Correct Spelling	Abbreviations	Incorrect Spelling
FIERY	FIRY = FIRY	FIREY
FILIPINOS	FNOS PHNS	PHILIPINOES
FLAMMABLE	FMMB FLMB	FLAMABLE
FORTHRIGHT	FOGT = FOGT	FORTRIGHT
FORTY	FOTY = FOTY	FOURTY
FULFILL	FUFL = FUFL	FULLFIL
GNAWING	GNWG KNWG	KNAWING
GOVERNMENT	GOVT = GOVT	GOVERMENT
GRAMMAR	GRMR = GRMR	GRAMMER
HEARTRENDING	HDNG = HDNG	HEARTRENDERING
HEMORRHAGE	HMGE = HMGE	HEMORRAGE
HINDRANCE	HNDN = HNDN	HINDERENCE
HYGIENE	HYGN = HYGN	HYGEINE
IDIOSYNCRASY	IDYY = IDYY	IDIOCYNCRACY
INCENSE	INNS = INNS	INSENSE
INCIDENTALLY	INDY = INDY	INCIDENTLY
INFALLIBLE	INFB = INFB	INFALABLE
INOCULATE	INOT INNT	INNOCULATE
INSISTENCE	INTN = INTN	INSISTANCE
INTERCEDE	INTD = INTD	INTERSEDE
INTERFERED	INFD INTD	INTERFERRED
JEOPARDIZE	JODZ JPDS	JEPRODISE
KIMONO	KMNO KMNA	KIMONA
LICENSE	LINS LINC	LISENCE
LIQUEFY	LQFY = LQFY	LIQUIFY
MAINTENANCE	MANN = MANN	MAINTAINANCE
MANAGEMENT	MMNT = MMNT	MANAGMENT
MANEUVER	MAVR = MAVR	MANUVEUR
MORTGAGED	MOGD = MOGD	MORTGAUGED
NICKEL	NIKL = NIKL	NICKLE
NINETYNINTH	NNTH = NNTH	NINTYNINETH
NOWADAYS	NWDY = NWDY	NOWDAYS
OCCASIONALLY	OCNY = OCNY	OCASSIONALY
OCCURRENCE	OCNE = OCNC	OCCURENCE
PAMPHLET	PAMT PHMT	PHAMPLET
PERMISSIBLE	PRMB = PRMB	PERMISSABLE
PERSEVERANCE	PRVN = PRVN	PERSEVERENCE
PERSUADE	PRDE PURD	PURSUADE
PHILIPPINES	PHNS = PHNS	PHILLIPINES
PITTSBURGH	PBGH PTBG	PITTSBURG
PLAGIARISM	PLGM = PLGM	PLAIGARISM
PLAYWRIGHT	PWGT PLWT	PLAYWRITE
PRAIRIE	PRRE = PRRE	PRARIE
PRECEDING	PRDG = PRDG	PRECEEDING
PRECIPICE	PRPC = PRPC	PRESIPICE
PREFERABLE	PRFB = PRFB	PREFERRABLE
PRESUMPTUOUS	PRMS = PRMS	PRESUMPTOUS
PRIVILEGE	PRVG = PRVG	PRIVELEGE
PROPELLER	PROR = PROR	PROPELLOR
PSYCHOLOGICAL	PSYL = PSYL	PSYCOLOGICAL
PUBLICLY	PUBY = PUBY	PUBLICALLY
PURSUER	PURR PRUR	PERSUER
QUESTIONNAIRE	QUTR = QUTR	QUESTIONAIRE
RECIPIENT	RPNT = RPNT	RESIPIENT
RELEVANT	RVNT = RVNT	REVELENT
RENOWN	RNWN RNUN	RENOUN
REPEL	REPL RPLL	REPELL
RHAPSODY	RHDY RADY	RAPHSODY
RHODODENDRON	RDDN = RDDN	RHODODRENDON
RHUBARB	RHBB RUBB	RUHBARB
RHYTHM	RHYM RYTM	RYTHM
SACRILEGIOUS	SAGS = SAGS	SACRELIGIOUS
SAFETY	SFTY = SFTY	SAFTY
SCISSORS	SCRS SIRS	SISSERS
SEIZE	SEZE SIZE	SIEZE
SEPARATE	SPTE = SPTE	SEPERATE
SHEPHERD	SHRD = SHRD	SHEPERD
SIMILAR	SIMR = SIMR	SIMILIAR
SINCERITY	SNTY = SNTY	SINCERETY
SOUVENIR	SOVR = SOVR	SOUVINER
SPECIMEN	SPMN SPMT	SPECIMENT
SUING	SUNG = SUNG	SUEING
SURREPTITIOUS	SUUS = SUUS	SUREPTITOUS
TRANSFERABLE	TRFB = TRFB	TRANSFERRABLE
UNPARALLELED	UNPD = UNPD	UNPARALELLED
USAGE	USGE = USGE	USEAGE
VEGETABLE	VGTB = VGTB	VEGATABLE
WEDNESDAY	WDDY = WDDY	WEDENSDAY
WEIRD	WERD WIRD	WIERD

(b)(3)-P.L. 86-36

REFERENCES

1. [redacted] "On the Recognition of Information with a Digital Computer," *Jour. ACM*, Vol. 4, No. 2 (April 1957), pp. 178-188.

2. [redacted] "Coding and Code Compression," *Jour. ACM*, Vol. 5, No. 4 (October 1958), pp. 328-330.

3. [redacted] and Friedman, E. A., "The Reconstruction of Mutilated English Texts," *Information and Control*, Vol. 1, No. 1 (September 1957), pp. 38-55.

Did Aleksandr Popov Invent Radio?

BY [redacted]

(b)(3)-P.L. 86-36

Unclassified

Popov vs. Marconi: a study of the evidence. The Russian claim to the invention of Radio is examined for the first time.

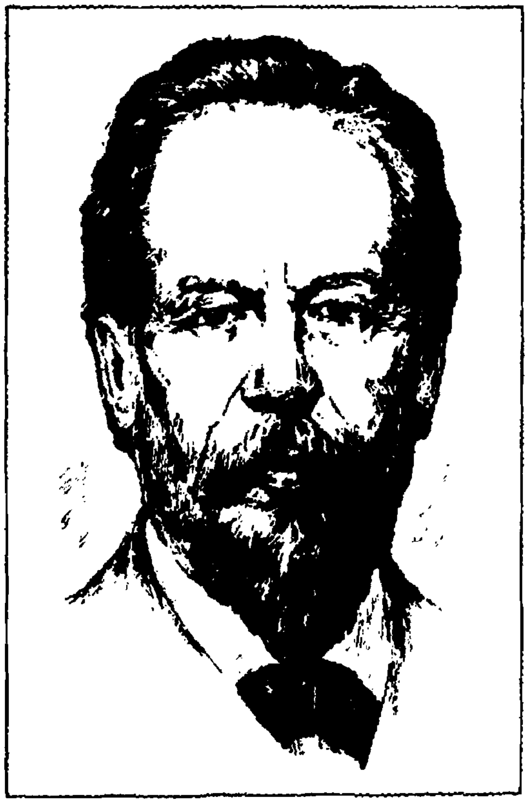
Ask an American who invented radio and he will probably say "Marconi"; ask a Russian and he will very likely say "Popov." Who is right? Can either Marconi or Popov be considered the inventor of radio? For that matter, who *is* Popov?

Throughout the Communist world Aleksandr Stepanovich Popov is recognized as the sole inventor of radio. A cursory examination of any recent Russian electronics journal makes this abundantly clear, for 1959 was the centennial of Popov's birth (he was born March 16, 1859[2] in what is now the Sverdlovsk oblast). To commemorate the anniversary, a number of special events were held during 1959; scientific meetings in Moscow and elsewhere; dedication of a statue of Popov in Leningrad; the Russian amateur radio organization held an international radio contest on Popov's birthday and offered a special award to any radio amateur who contacted 100 Russian amateur stations during 1959; special postage stamps have been issued, etc. Popov is memorialized in other ways, too. The Russian equivalent of the IRE is known as the Popov Society; scientists--both Russian and foreign--who make outstanding contributions to the radio art receive Popov gold medals; the first page or so of every Soviet book on radio-electronics is ritualistically devoted to a tribute to A.S. Popov, "the inventor of radio."

The Russian claim of priority in the invention of radio is based on an event of May 7, 1895 (since 1945 this day has been celebrated as Radio Day in the Soviet Union). At a meeting of the Physics Branch of the Russian Physical-Chemical Society in Petersburg, Popov, then an instructor at the Kronstadt naval school, reported on and demonstrated his invention, a "radio receiver." The device was actually designed only to receive and record lightning discharges; the term "radio receiver" (usually prefaced with "the world's first") became commonly applied to Popov's invention only after the advent to power of the Communists in Russia. This may be not so much willful distortion as it is a problem of definition. Popov's device *did* detect and record electromagnetic radiation (if only static crashes), and in that sense it *was* a radio receiver; yet, because there were no transmitting stations at that time, can his inven-

[1] This article has been accepted for publication in *Electronics World.*

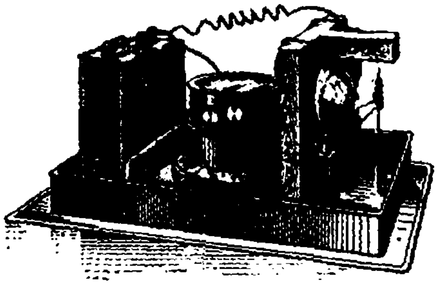
[2] All dates are New Style.



Aleksandr Popov
(1859 – 1906)

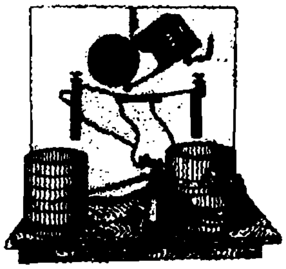
[redacted]

(b)(3)-P.L.
86-36



Popov's First Receiver

– [illegible] –



Popov's Lightning Detector (1895)

– [illegible] –

tion really be called a radio receiver?[3] In a way this is the reverse of the old question: "If a tree falls in the forest but there is no one there to hear it, is there any sound?" In 1895 there *was* someone to hear, but there was no *tree*, at least not near Petersburg.

While an instructor at Kronstadt, Popov had access to a well-equipped laboratory and a library well stocked with foreign periodicals and books. Popov was particularly interested in the work of Heinrich Hertz and he repeated many of the German's experiments in electromagnetic waves. The experiments and writings of Sir Oliver Lodge, Edouard Branly, Augusto Righi and others also influenced his thinking. The detector which Popov demonstrated before the Physical-Chemical Society meeting was basically Branly's coherer (a metal-filing type) to which Popov added an arrangement for automatically tapping back the filings to a sensitive condition after they had cohered upon reception of oscillations. Each static discharge caused a bell to ring or a mark to be made on a paper tape. The implication conveyed in some Soviet descriptions of Popov's receiver is that the tapping device was original with Popov. Actually, an automatic tapper was a part of Lodge's receiver demonstrated at a meeting of the British Association for the Advancement of Science in 1894. What may have been original with Popov was the addition of choke coils to protect the coherer from the effects of local sparking at the relay contacts.

Contemporary Soviet accounts of Popov's invention attach considerable importance to the antenna which he used with his receiver. Described as a long vertical wire, insulated at the upper end and connected through the coherer to ground at the lower end, it is claimed to have been the final element needed for the reception of radio signals. The literature is not conclusive on this point; Hertz had been using a loop antenna for his experiments, but whether Popov was the first to employ a vertical antenna remains an unanswered question. There is some evidence that Marconi had been using an antenna of this type in his experiments conducted at or before this time.

It should be pointed out that Popov foresaw that his invention might be used for purposes of communication. During his demonstration of May 7, 1895 he is reported to have said:

> With further improvement, my device can be adapted to the distant reception of signals by means of rapid electric oscillations, as soon as a sufficiently powerful source of such oscillations is found.

Perhaps unknown to Popov, a source of such oscillations had already been found. Early in 1895 (perhaps as early as the summer of 1894), at Pontecchio, near Bologna, Italy, a young man named Guglielmo Marconi

[3] Dictionary definition of radio: "The transmission and reception of signals by means of electric waves without a connecting wire . . ."

(b) (3)-P.L. 86-36 [redacted]

succeeded in receiving *and* sending wireless signals over a distance of about three-quarters of a mile. Similar experiments had also been made by Lodge and Sir Henry Jackson. From then on, progress was swift. Marconi moved to England and by the beginning of 1896 was receiving Morse code messages over a distance of nearly two miles. On June 2, 1896 Marconi applied for the first use of electric waves.[4] During 1896-97 transmitting distance was increased to four miles over land, then nine miles across the Bristol Channel. In 1899 wireless signals spanned the English Channel, the first instance of international radio communication. In the same year British warships, using Marconi equipment, exchanged messages at distances of 75 miles. Only two years later, on December 12, 1901, with Marconi at the receiving station in Newfoundland, the letter "S" was transmitted across the Atlantic. World-wide radio communication was now within reach.

What was Popov doing during this time? In January 1896 a report of his demonstration of the previous May was published in the Journal of the Russian Physical-Chemical Society under the title "A Device for Detecting and Recording Electric Oscillations." On March 24, 1896 Popov sent his *first* message by wireless. Transmitted over a distance of about 600 feet, the message consisted of two words: "Heinrich Hertz." Early the following year he was communicating with ships over short distances.[5] His equipment was employed in what was probably the first use of radio in the saving of human lives. In 1900 a message was flashed from Petersburg to the icebreaker *Ermak* instructing it to rescue some fishermen stranded on floating ice in the Gulf of Finland. In 1901, the year Marconi sent signals 2000 miles across the Atlantic, Popov established communication between ships on the Black Sea; the distance was about 80 miles.

How then can the Russians claim that Popov invented radio? Two arguments are used: (1) that Popov's demonstration of 1895 predated Marconi's patent of 1896, and (2) that, in any case, Marconi's invention was a direct copy of Popov's.

Popov is said to have refused to take out a patent on his invention, contending that the discovery should benefit the scientific world at large. This may be true (university professors are traditionally uninterested in patenting their discoveries), or it may be a convenient means of explaining how Marconi, rather than Popov, came to be almost universally recognized as the father of wireless communication.

With respect to the second argument, it is certainly true that no *one* inventor or invention was responsible for radio. And there was con-

[4] This was British patent No. 12,039. The equivalent American patent, No. 586,193, was granted him on July 13, 1897.

[5] A description of Marconi's wireless system was not published until June 1897.

siderable similarity between the inventions of Marconi and Popov, just as Popov's was similar to and based upon Lodge's, Lodge's upon Hertz's, etc. But this is really not the point. The thing that the Russians seem to overlook is that neither Popov, nor Lodge, nor Branly, nor Hertz really recognized the fact that radiation was the real key to wireless. And, as the courts later held, none of these scientists ever fully realized the practical possibilities of wireless as a means of communication. Marconi grasped both of these ideas. If not a creative inventor, Marconi was blessed with a genius for perfecting the crude laboratory-type apparatus of his predecessors and for promoting wireless telegraphy as a practical instrument of communication. He was, in short, the midwife of radio.

Without admitting that he was responsible for practical wireless telegraphy, Soviet sources, particularly the earlier ones, give at least some credit to Marconi for his contributions to the development of radio. A Soviet encyclopedia begins its article on Marconi by saying: "Marconi (1874-1937), Italian engineer and radio technician, the inventor, after Professor A.S. Popov, of the radiotelegraph." This 1940 source is kinder in its treatment of Marconi than one published in 1954. The latter dismisses Marconi as an opportunist who, taking advantage of the fact that Popov had not patented his invention, went ahead and obtained a patent on his device, which was, after all, only a copy of Popov's.

The contributions of the men who pioneered in the study of electricity and electromagnetic waves--Galvani, Volta, Morse, Bell, Faraday, Henry, Thompson, Branly and Lodge--are freely acknowledged, but in a condescending sort of way. The Russians take the attitude that what these men did was but prelude to Popov's "invention" of radio.

An interesting feature of Soviet accounts of Popov is that, of all the inventions claimed to have been made by Russians, radio seems to be the one first claimed. The argument that Popov was the real inventor of radio was put forth at least as early as 1938; other Russian inventions--including baseball and the hula hoop--were announced considerably later.[6]

There is no denying the fact that Popov's considerable talents were little appreciated by the tsarist government. It must have been particularly galling to Popov to see, in 1902, his rival Marconi decorated by the Tsar with the Order of St. Anne. There is no record that Popov ever received similar recognition by his government.

Popov's last few years were spent in Petersburg as a professor, then director, of the Electrotechnical Institute. He died on January 13, 1906 at the age of 47. The brain hemorrhage which caused his death was due, according to one recent Soviet source, to heated arguments between Popov and the tsarist minister to whom he was subordinate.

Returning to our original question, did Aleksandr Popov invent radio? No, and neither did Marconi. The latter made wireless practical, but without the pioneering work of scientists like (but probably not including) Popov, Marconi's achievements would have been impossible.[7]

An American scientist who recently visited the Soviet Union brings back an interesting anecdote. In a discussion of Russian claims that Popov invented radio, a Soviet electronics engineer is quoted as saying: "Well, Marconi did something, too, and what difference does it make? We now have radio and that's good!" And it is, too.

BIBLIOGRAPHY

Sources in English –

Dunlap, Orrin E., Jr. *Radio's 100 Men of Science.* New York, Harper and Bros., 1944.

Maclaurin, W. Rupert. *Invention and Innovation in the Radio Industry.* New York, Macmillan Co., 1949.

Marconi, Guglielmo. "Thirty-Seven Years of Radio Progress," *Radio News*, January 1932, pp. 551–54 ff.

Encyclopaedia Britannica. Chicago, Encyclopaedia Britannica, Inc., 1956.

Who Was Who. Vol. III (1929–1940). London, Adam and Charles Black, 1941.

Sources in Russian –

Izyumov, N. M. *Kurs Radiotekhniki (A Course in Radiotechnology).* Moscow, 1958.

Levinzon–Aleksandrov, F. L. *et al.* *Radiotekhnika (Radiotechnology).* Moscow, 1957.

60 Let Radio (Sixty Years of Radio). Ed. by A. D. Fortushenko, Moscow, 1955.

Voitkov, Fedor. *Rasskaz o Tvortsakh Telegrafa (The Story of the Creators of the Telegraph).* Moscow, 1950.

Bol'shaya Sovetskaya Entsiklopediya (The Large Soviet Encyclopedia). First and Second Editions, Moscow, 1938–1955.

[6] Popov is also credited with discovering the principles of radar and radio direction finding.

[7] While acknowledging the contributions of some of his predecessors and contemporaries, Marconi appears never to have recognized Popov's existence.

Book Reviews

Lost Languages, Philip Ellaby Cleator, London, 1959. Reviewed by [redacted]

(b)(3)-P.L. 86-36

The urge to discover secrets is deeply ingrained in human nature; even the least curious mind is roused by the promise of sharing knowledge withheld from others. Some are fortunate enough to be employed in the solution of mysteries, whether they be physicists who track down a hitherto unknown nuclear particle or policemen who detect a criminal. Most are driven to sublimate this urge, however, by the solving of artificial puzzles which have been devised for their entertainment. Detective stories or crossword puzzles suffice for the majority; the solution of secret codes may be the hobby (or the livelihood) of a few. *Lost Languages* is the story of the solution, primarily by cryptologic methods, of genuine mysteries which had baffled men for centuries; it is the story, too, of mysteries which still await their Champollion.

It was only a century and a half ago—a mere pinpoint in time—that certain discoveries were made in the humanistic sciences which paralleled the new and radical facts of knowledge in the fields of physical science and technology. It was in the 19th century that archaeology acquired a new look—a look based on the principles set forth earlier by Winckelmann; it was in the 19th century that there was an intensified study of original inscriptions and the first steps were taken toward a true science of linguistics. For the first time, men looked back at the races which had existed before the beginnings of Greek history and which had shaped the earliest history of mankind in the Near East; for the first time, scholarly attention was devoted to the inscribed monuments which had survived from the remote period of antiquity. Despite the Horatian dictum "*vixerunt fortes ante Agamemnona*" history had hitherto begun with Homer and the tales of the Old Testament; of earlier civilizations which had flourished elsewhere in the Mediterranean area, little was known, and the knowledge of ancient tongues was restricted to Latin, Greek and Hebrew. Admittedly, a certain formal familiarity with the monuments of ancient Egypt, perhaps even of Mesopotamia, had been salvaged from remote antiquity, but man still gazed at the odd pictorial or wedge-shaped characters with which these monuments were covered with the same sense of wonderment as had the Greeks and Romans, to whom the hieroglyphs were equally mysterious. Knowledge of these scripts had been lost in time, and seemingly no effort was made in late antiquity or during the Middle Ages to decipher them.[1] Thomas Paine perhaps reflected the vulgar feeling when he wrote in 1794: "As there is now nothing new to be learned from the dead languages, all the useful books being already translated, the languages are becoming useless, and the time expended in teaching and learning them is wasted. So far as the study of languages may contribute to the progress and communication of knowledge, it is only in the living languages that new knowledge is to be found."[2] And yet, today Egyptian hieroglyphics and language form part of our knowledge as well as the cuneiform characters of the Near East and many other formerly forgotten scripts and languages. Archaeological activities directed the attention of scholars to the countless inscriptions left behind by the early inhabitants of parts of Asia and Africa, with the result that we are today better informed about some of the monarchs who ruled these realms in 2000 B.C. than we are about events in England during the reign of Alfred the Great. The decipherment of these scripts and languages in the 19th and 20th centuries ranks with the most outstanding achievements of the human mind, and the only reason it does not stand in the limelight of public interest as a co-equal of the triumphs, in the same period, of physics and technology and their related sciences is that it cannot produce the same effect on practical daily life.[3] As a result of these achievements the historical horizon has been pushed back significantly, so that the surveyable history of mankind now comprises some 5,000 rather than 2500 years. This knowledge includes not merely political events but also the material and intellectual culture of these ancient races—their homes, their manner of living, their religious, juristic and scientific thinking; knowledge of the remoter past has made possible an insight into the development of human life and thought from a perspective far wider in space and time.

Philologists, prior to the initial decipherments, refused to admit that the incised and painted hieroglyphs of Egypt or the indentations exhibited by the baked clay tablets of Mesopotamia were a form of writing at all. *Lost Languages* tells how these and other age-old records came first to be discovered and then deciphered. In so doing it affords a fascinating glimpse of the cryptologist-decipherer and his work—the inspired guesses, the slender clues, the deductive reasoning, the apparently unrelated facts, the seemingly trivial details. It contains, in fact, the essential ingredients of an exciting detective story. Not only are linguistic remains, long defunct and forgotten, unearthed and identified, but they are effectively brought back to life. After a general introductory chapter on the diversity of tongues and the classification of languages, the author devotes a chapter each to the two great decipherments—the Egyptian hieroglyphs and cuneiform—and a chapter to what he describes as the subsidiary systems—Hittite, Ugarit and Minoan Linear B. In his concluding chapter he describes briefly the half dozen or more undeciphered scripts which, for one reason or another, continue to baffle scholars. A brief but informative history of the important nations or peoples concerned has been included in each chapter to provide the reader with the proper perspective, along with an account of the often bizarre individuals who each played his role in deciphering the linguistic puzzles. The gallery of portraits includes the brilliant Georg Grotefend, undertaking on a wager, if the story be not apocryphal, and with no real knowledge of the Oriental languages, to decipher the cuneiform script; Champollion, precocious genius, dedicated at twelve to unlocking the secrets of the hieroglyphs like a youthful Hannibal swearing eternal enmity to Rome; Michael Ventris, as a fourteen-year-old schoolboy, falling under the spell of the legendary Sir Arthur Evans and determining to take up the challenge of the undeciphered Cretan writings; the indefatigable Rawlinson copying the great Behistun inscription from a perilously swaying scaffold; and Young and Layard and Hincks and Lepsius and many others—along with a recognition of the existence and the toil of the uncounted Misses Blimber who labored mightily and reaped a mutely inglorious anonymity.[4]

It is in the details of the decipherment, however, that the cryptolo-

[1] In late antiquity, Horapollon in his *Hieroglyphica* advanced the view that the Egyptian script was not writing, like other writing, but concealed the secret wisdom of philosopher priests, to be understood only by one who had been similarly initiated into magico-mystic wisdom. This interpretation remained virtually unchallenged for centuries (attracting even Champollion) and explains why, as late as the 17th century, Athanasius Kircher in his *Sphinx Mystagogica* could give free rein to his imagination and interpret the simple phrase, "Osiris says," as "The life of things, after the defeat of Typhon, the moisture of Nature, through the vigilance of Anubis." If the absurdity of these hieroglyphic elucidations was not apparent to Kircher's admiring contemporaries, it was because the depth of his ignorance was more than matched by their own. Ironically, an accurate translation of the inscription of the so-called Flaminian obelisk had been made by Hermapion, an Egyptian priest, and preserved *in toto* for an incredulous posterity by Ammianus Marcellinus.

[2] *The Age of Reason*, I.

[3] This inferior evaluation accounts for the fact that the unlocking of the secrets of extinct languages and scripts is rarely described coherently and is, therefore, hardly known to the general public.

[4] "There was no light nonsense about Miss Blimber . . . She was dry and sandy with working in the graves of deceased languages. None of your live languages for Miss Blimber. They must be dead—stone dead—and then Miss Blimber dug them up like a ghoul." (Dickens, *Dombey and Son*, chapter 11.)

gist will be most interested, for it is obvious that there is a distinct similarity between an unreadable script and a secret code; similar methods may be employed to break both. The differences must not however, be overlooked. The code is designed deliberately to baffle the investigator while the script is only puzzling by accident. The language underlying the coded text is generally known; in the case of a script there are three separate possibilities. The language may be known or partially known but written in an unknown script; this, for instance, was the case with the decipherment of the Old Persian inscriptions by Grotefend in 1802; the cuneiform signs were then quite unknown, but the language, as revealed by the recognition of proper names, turned out to be largely intelligible through the medium of the Avestan texts. Secondly, the script may be known while the language is unknown. This is the case of Etruscan, which is written in a modified form of the Greek alphabet presenting little difficulty to the understanding of its sounds, but as yet no language has been found closely enough related to throw any light on the meaning of the words. Thus, in spite of a large collection of inscriptions our knowledge of Etruscan is still very elementary and uncertain. Finally, there is the situation which confronted the decipherers of the Minoan script—an unknown script *and* an unknown language. The fact that the language *subsequently* proved to be known is irrelevant; that fact could not be used in the first stages of the decipherment. In this last case decipherments have usually been judged to be possible only when they could start from a bilingual text. The Egyptian hieroglyphs began to yield their secrets only when the discovery of the Rosetta stone, with the Egyptian text repeated in Greek, made it possible to equate the royal names in the two versions.

It is apparent that cryptology has contributed a new weapon to the student of unknown scripts. It is generally known that any code can, in theory, be broken, provided sufficient examples of the coded text are available; the only method by which to achieve complete security is to ensure continuous change in the coding system or to make the code so complicated that the amount of material necessary to break it can never be obtained. The detailed procedures are irrelevant, but the basic procedure (obvious to the reader) is the analysis and indexing of coded texts so that underlying patterns and regularities can be discovered. If a number of instances can be collected, it may appear that a certain group of signs in the coded text has a particular function; it may, for example, serve as a modifier. A knowledge of the circumstances in which a message was sent may lead to other identifications, and from these tenuous gains further progress becomes possible until the meaning of most of the coded words is known. The application of these basic cryptologic methods to unknown languages is obvious; such methods enable the decipherer to determine the meaning of sign groups without knowing how to pronounce the signs; indeed, it is possible to imagine a case in which texts in an unknown language might be understood without finding the phonetic value of a single sign.

Certain minor criticisms of *Lost Languages* may be made, even though the author makes no pretense of having written anything other than a reasonably accurate popular account of a subject far too little known. C. W. Blegen of the University of Cincinnati consistently appears as Blegan; a scholar famous in the field of ancient history and especially renowned for his archaeological discoveries at Troy and Pylos surely deserves to have his name spelled correctly. To the bibliography, part of which is out of date and part of which appears to be mere padding, should be added Pallottino,[5] Bloch,[6] Friedrich[7] and Chadwick[8]—the last, especially, of great interest to the cryptologist. From the standpoint of the cryptologist, too, I should suggest that a complete chapter might well have been devoted to the decryption of Minoan Linear B which Gelb, at the Second International Congress of Classical Studies at Copenhagen in 1956, described as the "most successful single attempt in the whole history of the decipherment of unknown writings and languages."[9] Admittedly, one may always read Chadwick, so that this complaint, like the others, may be captious and unjustified.

What are the prospects for the future? The very fact that Ventris' astounding feat was accomplished as recently as 1952 by someone other than a professional philologist certainly suggests that there is nothing to prevent would-be Champollions from exercising their ingenuity and talents, always providing that these attributes are accompanied by a thorough knowledge of the subject of their choice. Not a few problems are at present outstanding, some of them far from new, as, for example, that presented by the language of the Etruscans, which has long puzzled scholars and is apparently little nearer solution than it was 2000 years ago.[10] Other questions have arisen since the beginning of the present century, and some of them, at least, promise to be less intractable since they seemingly await nothing more than

[5] Pallottino, Massimo, *The Etruscans*, Rome, 1954.

[6] Bloch, Raymond, *The Etruscans*, New York, 1958.

[7] Friedrich, Johannes, *Entzifferung Verschollener Schriften and Sprachen*, Berlin, 1954.

[8] Chadwick, John, *The Decipherment of Linear B*, Cambridge, 1959.

[9] With the possible exceptions of Beattie and Grumoch, scholars now accept the accuracy of Ventris' decryption.

[10] Perhaps the incipient Etruscan club within our midst may rend the veil.

the discovery of additional material. Gordon, at Brandeis, claims to have identified Linear A terms with words used in Babylonian Akkadian; others have speculated on possible Semitic affinities, and the ultimate solution may be found along these lines even though these views still appear premature to the scholarly community. What harm the bigotry of the vandal cleric de Landa wrought in destroying almost completely the ancient Mayan records may happily be righted by the activities of the Friedmans who even now are investigating the Mayan glyphs in an attempt to decipher something more than the calendrical texts; this may well be a difficult task since it seems unlikely that the Mayan writing is a phonetic system, if only because it has so far defied all attempts at elucidation even though Mayathan continues to be spoken in the neighborhood. These and other problems, however, will yield in time to persistent investigation, as have all the seemingly unsolvable problems of the past. Whatever the language, however obscure, each additional achievement will advance in its own way the sum of human knowledge.

———R. F. B.

* * *

Aristocrat—An Intelligence Test for Computers

BY H. CAMPAIGNE

~~*Confidential*~~

The solution of monoalphabets was demonstrated on BOGART. This demonstration was interesting because it shows the power of BOGART, and because it forges another link in the chain of techniques needed for total automation.

Among puzzle addicts it is admitted that monoalphabets are the aristocrats of puzzles. In fact, a particular type of monoalphabet has come to be called an *aristocrat*, distinguished by its short text, spaces between words, and a bizarre vocabulary.

In cryptanalysis, monoalphabets are encountered in many places. They occur in busts when some changing element fails to change. Many cryptanalytic procedures have the solution of a simple substitution as a final step, the previous more sophisticated steps leading to an unknown wiring of a wheel or plugboard. And finally, monoalphabets are interesting in themselves as the simplest of all ciphers.

These two interesting aspects of substitutions become fascinating when viewed in the light of another recent development, the exploration of the flexibility of computers. Digital computer applicability to all kinds of problems is highly touted, but little is known about its limitations. For ten years claims have been made for language translation on computers, but only recently have any translations appeared. The quality of these translations is a matter of discussion; since there are no objective standards for accuracy and smoothness of literary works, these are described variously as "miserable," "usable," and "all that one could ask." So it is still not known how effective the computer will be. It is very rare to find a problem which it is known that a computer cannot solve; in most cases it is thought the computer could produce answers if it were programmed. Of course a computer cannot play tennis, nor weed the garden, nor do other obvious things. But the boundaries of computer ability have yet to be found.

The use of machines to aid cryptanalysis has been extensive at NSA. In some cases, problems have been carried almost from intercept copy to plain text entirely by machine. But of all the mechanization very little is on simple substitution. This is partly because people have not needed help, and partly because mechanization is difficult, surprisingly more difficult than for other "more sophisticated" operations.

The question posed here is: *How effectively can a machine solve simple substitutions?* which resolves immediately to: *How can a computer program be written to solve simple substitutions?*

This question I have attacked through a program called "Aristocrat." This was an adventure with many interesting aspects.

There are many versions of the problem. Will the cryptogram be spaced into words? If not, will it be spaced into groups? [redacted]

The techniques to be applied can depend on the kind of plain text underlying the messages. Success is heavily dependent upon one's ability to predict text. What kind of plain text will we have in our problems? A series of messages about a military operation can be very redundant, full of "arrivals" and "departures," "reconnoitering" and "attacking." On the other hand, puzzles rely on having the most unpredictable text; "veal sables salute snooty ladies." Aristocrat was aimed at doing the problems in *Military Cryptanalytics, Part I*, specifically those with one hundred letters of text.

The number of techniques for attacking cryptograms is very large. [redacted]

Aristocrat could easily become a major project. As it exists now, it suffers from many arbitrary restrictions imposed to save time or memory. [redacted]

[redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

In summary then it seems that my shortcomings as a programmer rather than those of Bogart as a data manipulator have been probed. Aristocrat can read some of the cryptograms in Friedman and Callimahos. It could be made more flexible and more powerful, and I know how to do it if there were time, and that is by providing for a number of additional contingencies. [redacted]

THE ARISTOCRATIC PLAN

[redacted]

[redacted]

CRITIQUE

[redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[redacted]

Fig. 1.

Copy No. 173

~~TOP SECRET~~ Non - Responsive

NSA TECHNICAL JOURNAL

VOL. VII SPRING 1962 NO. 2

Page

[redacted]

[redacted]

WARNING

~~This Document Contains CODEWORD Material~~

~~TOP SECRET~~

EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

[redacted]

Non - Responsive

A Cryptologic Fairy Tale

BY BRIGADIER JOHN H. TILTMAN

~~Top Secret Dinar~~

The paper describes the diagnosis and solution in 1939 of a German Transposition field cipher and traces the derivation from it of a British field cipher and further development therefrom of the main German Army field cipher of 1944 1945, the "Rasterschluessel". The principles of the security of transposition systems are discussed.

I am afraid that the title of this paper gives you very little idea of its subject. The title, however, is not as unreasonable as it sounds. In the first place the subject is definitely "cryptologic" as it has both cryptographic and cryptanalytic aspects. Further, it can be called a "Fairy Tale" for two reasons:

(1) It departs somewhat from the truth because the workings of the cryptanalytic solution which forms the first part of the lecture have not survived and I have had to construct an example exhibiting features as close to the original as I could from memory, and

(2) The story has a reasonably happy ending.

I couldn't think of a title that would express the essence of the subject less cumbersome than the following:

"Cross-pollination of cryptographic ideas between enemies."

The naval, military and air sections of GCHQ moved to their war station, Bletchley Park, on 15th August 1939 a couple of weeks before the Germans invaded Poland. I was in charge of the military section. About the middle of September we received some intercepts presumed to emanate from German Panzer units in action in Poland, which showed the following superficial characteristics. No message exceeded 138 letters in length, of which the first 8 letters clearly constituted a non-textual indicator of some kind, the first digraph being repeated as the second and the third repeated as the fourth. The remaining letters of the message conformed to German literal frequency. The system employed could therefore be assumed to be some form of transposition.

[redacted]

[redacted]

[redacted]

EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

[redacted]

[redacted]

[redacted]

There is not sufficient information in my fabricated example to derive the indicating systems completely but the general lines can be deduced. In the original German system, called by them the *Heftschluessel*, the 26 letters of the alphabet were rearranged at random and written in two lines of 13 letters each at the top of the grille and again at the left hand side, giving two alternative letters in each position. The two transposition keys were written at the top and bottom of the grille respectively. The first digraph (repeated for check purposes as the second) gives column and line coordinates for the starting point of the plain text within the grille. The third digraph (repeated as the fourth) gives the starting points within the two keys used cyclically.

In the German usage of this system the transposition keys were changed daily, also presumably the two alphabets used for the indicators. I don't remember how often the grille was changed but it certainly was not constant for all key-areas or for long periods. Shortly after the solution of the messages intercepted during the invasion of Poland, the same system became heavily used for a totally different purpose. An Army transmitter somewhere in western Germany began broadcasting at 4-hour intervals [redacted] messages known as *Barbarameldungen*. These proved on solution to be corrections for weather conditions to artillery range-tables. Regularly 2 hours later than each of these [redacted] messages the same station sent out long general weather forecasts and these were enciphered in the *Heftschluessel*, and, owing to the limitation of textual message-lengths to 130 letters, each of them was enciphered and transmitted in 5 or 6 (sometimes even 7) parts. This meant that we received between 30 and 40 messages a day. [redacted]

However, after we had managed to recover the daily changes for rather more than a month, the system was changed. The successor cipher had a similar indicating system and was clearly a transposition cipher but the number of textual letters in a message was limited to 120 instead of 130. The weather forecasts continued to come in in several parts 6 times daily in the new cipher and [redacted]

[redacted]

On 1st February 1940 this new system went out of use and was replaced by the first German Military Double Playfair System which I managed to break into in about 2 weeks, thereafter reading more or less currently for about two months.

During 1940 and 1941 I was under continuous pressure to give attention to the cryptographic security of transposition systems. There were three reasons for this:

(1) The German police were using Double Transposition [redacted] [redacted] for each day for the first and second processes respectively.

(2) The British Army was using a Grille Transposition System known as the Army Stencil Cipher whose security I had criticized on the grounds that the stencil carried too many holes, c.s. permitted squares. The *Heftschluessel* whose solution I described earlier is an example of this, the proportion of 3 forbidden to 10 permitted squares [redacted]

(3) I had to provide a cryptanalytic training course at short notice to test the capability of new recruits to GCHQ before they were accepted and placed in the organization.

[redacted]

Here is a special case you may not all have seen. This is not part of the fairy-tale—it really happened. During the first course of the Cryptanalytic School I started in Bedford in 1941, the Chief Instructor, Major Masters, was giving a first description of the process of Double Transposition on the blackboard. He chose a short key at random and wrote it on the board—53142. He then wrote a short message under it

```
53142
ARRIV
INGTO
DAY
```

He then wrote the key down again and wrote under it horizontally the columns of his earlier diagram in numerical order:

```
53142
RGYVO
RNAIT
AID
```

He then took out the columns in numerical order and wrote them horizontally: YADOT GNIVI RRA, this being his original text written backwards.

[redacted]

Sometime later in 1941 I produced the "Cysquare" which was accepted by the War Office as a low-echelon cipher to replace the "Stencil" cipher and issued to the Eighth Army in North Africa. Figures 8 and 9 give photographs of two pages of the printed instructions. The grille has 676 (26 x 26) squares. Each column and each line contains 10 white (permitted) squares, with the exception of 3 "plus" lines containing 20 white squares each and 3 "minus" lines which contain no white squares at all. The key for the day consists of 26 letters of the alphabet in random order with the numbers from 1 to 26 written under them also in random order. For each message the operator selects a 4-letter indicator from a random list of such groups provided him for use in turn. The indicator in the case of the example given is GMBX. The numbers corresponding to this indicator are 11 19 20 7, *i.e.*, position 11, line 19, column 20, taking out number 7. The grille could be used with any of its sides at the top. Position II indicates that the grille is used as shown with numbers 8 to 13 at the top. The numerical key for the day is written from left to right at the top of the grille and from the bottom upwards on the left hand side. The plain text is written into the grille starting at the next white square after the square described by the line coordinate 19 and the column coordinate 20, using the elements of the key to define the corresponding lines and columns. If and when the operator reaches the last white square in the grille he proceeds from the top left-hand corner. He then takes out the columns of letters starting at the top of the grille and in the column designated by the taking out number, *i.e.*, in this case 7. The message is written out in 4-letter groups preceded by the 4 letter indicator and followed by the number of letters, the indicator repeated, and the time and date. No message of more than 220 letters was permitted. If a message handed in for transmission exceeded this length it had to be divided into parts, none of them exceeding 200 letters in length.

The cipher was originally designed to be used in one of two forms:

(1) *Stencil form*, in which holes were punched through a card to correspond to white squares. This form allowed both sides to be used, giving 8 "positions" instead of 4.

(2) *Pad form*. Here the grilles were issued in pads of 50 pages each printed with identical grilles. I note from the instructions (which I did *not* write) that the operator was encouraged to use each sheet as many times as possible by rubbing out the letters of each message after use!

Everyone who has had the responsibility of designing a cipher knows that a cryptographic system has to be a compromise between security and practicability. I consider my Cysquare to have been strong on security!

At this point I may as well confess that the cipher was a complete flop. It must have been issued to the Eighth Army in pad form as it was apparent very shortly after its introduction that the code clerks refused to use it on the grounds that after a very little desert weather and use of indiarubber the permitted squares were indistinguishable from the forbidden ones. The failure of the cipher created a temporary communication vacuum which had to be filled in another way, but, in the meantime, whenever Rommel overran British armoured and infantry units he captured the Cysquare with its instructions and the German cryptographic experts apparently thought it was wonderful.

[redacted]

[redacted]

[redacted]

EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

Fig. 1.

EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

[redacted]

EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

Fig. 3.

Fig. 4.

EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

Fig. 5.

[redacted]

EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

EO 1.4.(b)
EO 1.4.(c)
EO 1.4.(d)

Fig. 9.

(b) (3)-P.L. 86-36

Why Analog Computation?

BY [redacted]

Unclassified

An introduction to analog computation containing a brief description of the analog computer and problems in which it can be advantageously applied. Both analog computers and systems combining analog and digital techniques are discussed in order to show why the Agency's interest in this computation area has increased.

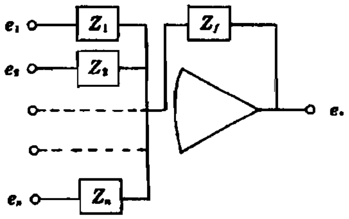
Why analog computation? With the interest in analog computing equipment rapidly increasing in our digitally oriented Agency, this is a question many of us must ask. The preponderence of digital computing equipment in this Agency would preclude analog computation from consideration if the two types of computers performed the same operations equally well; but this is not the case. A comparison of digital and analog computer applications reveals a basic difference in their operation. The digital computer performs numerical operations on discrete signals; in contrast, the analog computer performs algebraic and integro-differential operations upon continuous signals. Therefore certain operations, which are difficult to program on a digital computer, are available inherently on the analog machine. In order to appreciate where an analog computer can be advantageously applied, one must become more familiar with what it is and how it is used.

Before discussing problem areas in which the analog computer possesses an advantage, let us briefly consider the fundamentals of its operation.

The heart of the computer is the high-gain D.C. amplifier—either vacuum tube or transistor—that, when properly connected with passive components, forms the basic operational element. The schematic representation for an operational amplifier is shown in Fig. 1.

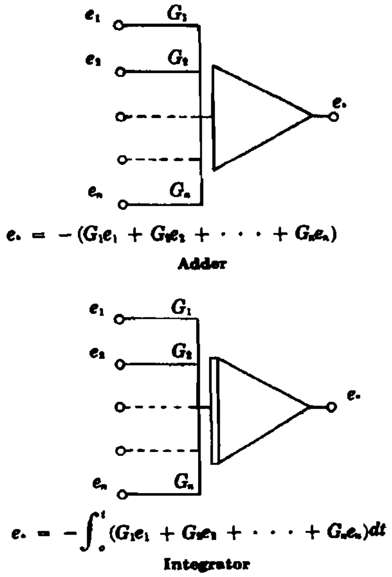
If the passive components in both feedback and input arms are entirely resistive, the circuit of Fig. 1 adds the applied voltages in proportion to the ratios of the individual resistors; while if the feedback impedance is capacitive, the circuit integrates the sum of the applied voltages. The schematic diagrams for an amplifier used as a summer (it is called an inverter if it has only one input) and as an integrator are shown in Fig. 2.

(b)(3)-P.L. 86-36



$$e_o = -\left(\frac{Z_f}{Z_1}e_1 + \frac{Z_f}{Z_2}e_2 + \cdots + \frac{Z_f}{Z_n}e_n\right)$$

Fig. 1.—**Operational Amplifier.**



$$e_o = -(G_1e_1 + G_2e_2 + \cdots + G_ne_n)$$

Adder

$$e_o = -\int_0^t (G_1e_1 + G_2e_2 + \cdots + G_ne_n)dt$$

Integrator

Fig. 2.

If the simple input and feedback impedances are replaced with complex networks, either passive or active, the amplifier circuit will develop more complicated transfer functions than those shown in Fig. 2. In addition to the basic amplifiers, the general-purpose analog computer usually contains a variety of special purpose units; for example, multipliers to form the product of two or more variables, fixed and variable-diode function generators to perform various nonlinear operations on the variables, switches to start and modify the operations, and comparators to make elementary decisions based on the value of a particular variable. It is the compatability and simplicity of interconnection of these various components that give the analog computer its flexibility and versatility.

With this brief discussion of the analog computer itself as background, the solution of problems with it will be considered. The analog computer has basically two modes of operation. The first mode is a simulation of the mathematical equations that describe a system; while the second is a simulation of the functions that a system must perform in processing continuous signals "on line". The first mode is used when the basic parameters of the system are to be investigated; the second, when its total characteristics must be evaluated. The choice of the simulation technique to be used for a particular problem usually depends on the nature of the solution required. Either mode of simulation or a combination of some features of both may yield the most fruitful results depending upon the degree of interest in the detailed operation of the specific parts and the overall operation of the entire system. For simulation on the analog computer, it is not necessary that a problem be electrical in nature since the solutions are obtained from an analogy between the physical variables—be they electrical, mechanical, mathematical or the like—and the computer voltages. After a problem has been simulated, care must always be exercised in checking trial solutions against experimental or analytical data to insure that the solutions do satisfy, at least at some particular points, the original statement of the problem.

Although a detailed simulation obtained from the defining equations offers many advantages in the analysis of the operation of a system, only a few of the more general ones will be discussed here. The first advantage is that the individual parameters may be isolated on the computer so that each may be varied independently; and, therefore, the required response function may be optimized systematically. This mode of operation has particular appeal for the electrical engineer since the machine simulation may be used in the same manner as the "bread board" circuits to which he is accustomed, but with increased flexibility and more rapid and simpler modification of

(b)(3)-P.L. 86-36

[redacted]

the parameters than with the actual circuit. A second advantage is that, since ideal elements can be substituted in the simulation for the physical components, information can be obtained about the parameters that can not be gotten by direct measurement on an actual circuit. Still another advantage is that the solution of non-linear problems is only slightly more difficult than the solution of linear ones; in fact, a non-linear problem is usually programmed as a linear one, and then the non-linear function is inserted in place of its linear approximation. In this manner the non-linear problems, that resist analysis in all but the simplest cases, can be solved quite readily on the analog computer with little additional effort.

To illustrate this mode of operation, the following problem of particular current interest to the agency is discussed. Various tunnel diode circuits are to be evaluated in order to determine those which look most promising for use in high speed digital computers and similar applications; and then these circuits are to be investigated in greater detail to develop design criteria. To analyze each proposed circuit on the analog computer, a circuit diagram is drawn using a linear model for the tunnel diode; and from this circuit are written the system equations. Although the analog computer does not operate at the same speeds and voltage levels as the tunnel diode circuits, it can be made to represent their operation by the proper time and amplitude scaling of the equations. After the linear equations are programmed for solution on the computer, the negative resistance characteristic of the diode, as shown in Fig. 3, may be set up on a variable-diode function generator and inserted in the program in place of the linear resistance.

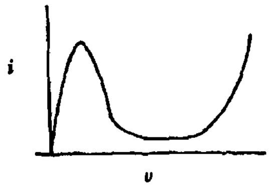


Fig. 3.—Tunnel Diode Characteristic.

The most direct application for this non-linear simulation is the investigation of the affect on the circuit response caused by varying the linear components, with the diode characteristic held constant, because these components can rapidly be modified by changing with potentiometers the gain of the amplifiers that represent them. In addition, the diode characteristic itself may be easily modified to conform to any specified values that correspond to a particular diode's parameters, or to parameter values that are not now available in actual diodes but that appear to offer some potential advantage in the circuit. This brief discussion illustrates some of the advantages that the analog computer possesses in the solution of this class of problems.

The simulation of the functions that a system must perform in processing continuous or, as they are sometimes called, analog signals is also readily accomplished on the analog computer. A simple example of an analog system is a radio receiver since it must filter, amplify and demodulate continuously incoming signals. All these operations can be simulated on a general purpose analog computer by interconnecting the components available. For the processing of limited bandwidth signals such as speech, the computer is capable of operating directly upon the signal, or a tape recorded copy of it; but for wider bandwidth signals, such as those encountered in a radio receiver, it is necessary to expand the time scale of the simulation and operate upon slowed down or simulated signals. The advantage of simulating a system, either in real or expanded time, on the analog computer is that instead of constructing a special-purpose equipment just to determine the efficacy of a proposed scheme in processing some particular data, the standard components on the computer can be rapidly connected and tested. If the simulation reveals that the process justifies the construction of a special-purpose machine, the simulation can then be used to compile information about the various system parameters that can be used to simplify the design of the final machine.

To illustrate this type of simulation the following example on correlation is presented. Since the correlation function is a measure of the similarity of two signals, in many instances it would be advantageous to accomplish this comparison "on line", as rapidly as possible, so that the resulting information may be used to make an immediate decision. In order to avoid a lengthy discussion of the correlation process itself, the problem will be stated simply as the determination of the correlation function defined by the following equation:

$$R_{12}(\tau) = 1/T\int_0^t X_1(t)\,X_2(t+\tau)\,dt$$

If X_1 and X_2 are the same signal, this is called an autocorrelation function; and if they are different signals, it is a crosscorrelation function. This equation indicates that a product must be formed of the two signals at various offsets in time (τ) and that each product must then be integrated over the specified interval to determine the correlation function. For solution on a digital computer it would be necessary to sample and store the two waveforms, multiply the corresponding samples for each offset, and then numerically integrate all the resulting products. Since a very large number of samples is necessary to accurately represent most signals, even the most modern digital computers would have difficulty in performing all the required operations rapidly enough to make the decisions "on line." In contrast, analog equipment—either optical or electronic—which includes delay lines can instantaneously multiply the two signals as received and integrate the product for the various offset signals obtained from the delay line. The analog computer can prove extremely useful in evaluating the effectiveness of correlation in producing the required information because it contains the multipliers and integrators needed for testing the process, and delay lines can be simulated when an expanded time scale is used. Although the limited bandwidth of the operational amplifiers restricts the class of signals that can be correlated directly on the analog computer, some analysis of speech is within the capabilities of present analog computers. Although higher frequency signals can not be correlated directly on the analog computer, they can be investigated either by reducing their speed on a tape recorder or using simulated waveforms in place of the actual signal.

Now that the application of an analog computer to typical problems has been discussed, let us again compare it to a digital computer. The analog computer readily solves problems with a single dependent variable. Usually this variable is time, but others can be programmed. In contrast, since the operation of the digital computer is unaffected by the number of independent variables in the problem, it can be programmed with a greater degree of flexibility than the analog computer when more than one independent variable is present in a problem. The cost of increasing the accuracy with which the digital computer calculates a particular value is only time, while the analog computer would have to be reconstructed of more exact components to increase its accuracy. Therefore, if extreme accuracy is needed at each point, the digital computer is the best device; but remember that it provides no information between these points, while the analog computer, though less exact, has a continuous solution. The fundamental differences in the two types of computers have led to machines that combine some features of each in a hybrid system.

The oldest of these combined machines is the Digital Differential Analyzer. This machine is actually a special-purpose digital computer that is programmed like an analog computer and not with a stored set of instructions. In this machine a group of numerical integrators replaces the operational amplifiers of the analog computer as the basic computing element. Since these numerical integrators can be connected in parallel on the Digital Differential Analyzer, it can solve a set of equations more rapidly than a general-purpose digital computer, although still not as quickly as an analog computer. With this parallel operation, it is possible to obtain solutions more rapidly, while still taking advantage of the digital computer's greater accuracy. A more recent development has been the iterative analog computer which incorporates digital circuitry to provide logic and storage. Iterative computers may be programmed to operate faster than real time and obtain the solution repetitively; electronic switches are then employed to store the results of one solution and use these results as initial conditions for the subsequent solution so that the problem may be solved iteratively. The inclusion of *logical control* of the switches enables the programmer to use several different solution rates in a single problem and thereby handle problems of more than one variable. The compressed time scale—faster than real time—permits the simulation of systems in which the uncertainties are known only in a probabilistic sense and therefore require statistical analysis. The compressed time scale allows an adequate number of samples to be taken in a reasonable length of time so that meaningful statistics afe obtained. A third approach to combining the best features of each type of computer has been to design circuitry which couples two standard computers. This additional equipment permits communication between the two computers by providing intermediate storage and conversion between the analog and digital variables of the individual machines. This approach offers the greatest flexibility in programming at the cost of data conversions that are not required in the special-purpose machines previously discussed. Whether to use a hybrid system or one of the basic machines depends, of course, on the nature and complexity of the individual problem.

It is hoped that this paper has provided some insight into why the Agency's interest in analog computation has increased. Since analog computation possesses advantages in some problem areas, it is necessary to investigate both analog computers and hybrid systems in order to provide the most efficient means of computation for Agency problems.

PROFESSIONAL READING: Books Briefly Noted

Pearl Harbor: Warning and Decision, by Roberta Wohlstetter, Stanford, 1962.

This is one of the most thorough analytical studies of the events leading up to any war and will probably become *the* book on the controversial question of the surprise attack on Pearl Harbor. The author, with commendable objectivity, carefully documents from open source material an incredibly complicated story and enables even a casual reader to understand the workings and difficulties of pre-war intelligence operations. Nearly sixty pages of the book are devoted to MAGIC, the name applied to the process by which United States experts decoded Japanese secret diplomatic messages. In the clearest exposition of the subject which has yet been published, Mrs. Wohlstetter develops the thesis that the necessity for extreme secrecy in the use of MAGIC often made it impossible for proper evaluations to be made of the material. By getting at the publicly available facts, piece by piece, and by analyzing them and arriving at logical conclusions, the author has become the leading authority on Pearl Harbor. *Pearl Harbor: Warning and Decision* is without doubt the best published treatment of this highly controversial incident in American History.

* * *

But Not in Shame, by John Toland, Random House, New York, 1961.

The title of this book is taken from General Wainwright's last message to President Roosevelt, the first paragraph of which reads:

> With broken heart and head bowed in sadness *but not in shame,* I report to your excellency that today I must arrange terms for the surrender of the fortified islands of Manila Bay.

It is the extraordinary story of the first six months of the war with Japan and is based primarily on interviews by the author with hundreds of surviving participants in those stirring events. Of particular interest to Agency personnel is the vital role played by cryptanalysis in containing and hurling back the Japanese advance. Japanese leaders, prior to the Coral Sea operation in May 1942, still did not have the slightest suspicion that the "Purple" code had been broken months before by a team of U.S. cryptanalysts and that, in consequence, Admiral Nimitz was aware of the impending attack on Port Moresby. Later in that month, decoded Japanese messages warned of the impending Midway operation, referring, however, to the point of attack merely as "AF." Washington believed that "AF" referred to Oahu while Admiral Nimitz was convinced that "AF" meant Midway. Eventually, Midway was ordered to send a fake, uncoded message reporting the breakdown of the distillation plant there. Two days later, cryptanalysts in Pearl Harbor's "Black Chamber" decoded an intercepted Japanese dispatch which revealed that "AF" was low on fresh water. With the certain knowledge that Midway was Yamamoto's target, the United States was able to inflict a crushing defeat on the Japanese Navy and to conclude with a decisive victory the first six months of the Pacific War.

* * *

The Secret War, by Sanche de Gramont, G. P. Putnam's Sons, New York, 1962.

The author's credentials, at least, are impressive: winner of a Pulitzer Prize in 1961; student at Yale, Columbia and the Sorbonne; service with the French Army in Algeria; reporter for the Worcester *Telegram* and later for Agence France Presse as well as the Associated Press; and now a foreign correspondent, based in Paris, for the New York *Herald Tribune*. The story he tells is, essentially, a story of the spy trade and is told with candor, perspicacity and reasonable precision. Nearly half the book is devoted to individuals—Judy Copland, Harry Gold, Klaus Fuchs, Rudolf Abel, Martin and Mitchell and Burgess and Maclean, George Blake, the Krogers along with many others—but he has not neglected the organizations for which they work. The book reveals, theoretically, some of the inner working of CIA, the KGB (Committee for State Security in the USSR), NSA, and the GRU (Overseas Intelligence Branch of the Red Army). The author discusses, with equal objectivity, the faults and merits of these organizations, their successes and failures, their philosophies and operations. One might be surprised to learn that the NSA building ("a monument to planned intelligence") possesses the longest unobstructed corridor in the world—980 feet long and 560 feet wide, that it is protected by four gatehouses manned by guards armed with machine guns, that its battery of computers includes the new Whirlwind which is said to be able to break any code, and that wastebaskets are provided with paper linings, specially marked for each office, which are stapled at the end of the day and stored for a specific period to ensure that nothing has been discarded by mistake. One may smile, but, even allowing for certain lapses, the book is interesting and informative, whatever doubts one may entertain about the author's reliability after reading his account of NSA.

CIA—The Inside Story, by Andrew Tully, William Harrow and Company, New York, 1962.

To the uninitiated—and their number is legion—the inner workings of CIA are confused, impenetrable and baffling. Even to those who have at least some knowledge of the operations of other government agencies, CIA and its doings remain enigmatic—and appropriately so, for the collection, analysis and distribution of intelligence must, by its very nature, be cloaked in secrecy and mystery. *CIA—The Inside Story* pulls aside the cloak a trifle, revealing its history, its methods, its trials and tribulations, and the problems which it encounters both at home and abroad. It reveals the role of the agency in such activities as ousting Arbenz from Guatemala, in engineering the coup against Mossadegh in Iran, in assisting in the capture of Abel, and, as a climax, in the debacle of the Cuban invasion of 1961. Well written and generally objective, this book is informative and well worth the time of anyone who is interested in the more devious aspects of present day political activities. It indicates, too, how far the U.S. has come in the business of espionage from the days when Mr. Stimson dissolved the State Department's code breakers' office because "gentlemen don't read other people's mail."

* * *

Now It Can Be Told, by Leslie R. Groves, Harper and Row, New York, 1962.

"Never in history has anyone embarking on an important undertaking had so little certainty about how to proceed as we had then." Thus does General Groves describe the situation in the early days of the Manhattan Project. In this book he reveals the story—based on documents, most of which have hitherto been available only to him—of Oak Ridge, the intelligence search for atomic information in Europe, the negotiations with the British and the Belgians for the exchange of information and raw material, Hiroshima, Nagasaki, and eventually the transition to peacetime management. In answer to the question whether it is worthwhile, after nearly twenty years, to study the Manhattan Project in detail, General Groves explains his reasons for this account: to fill in the gaps still existing in the public understanding of the project; to emphasize the cohesive entity that was the project—a major factor in its success; and, finally, to record the lessons learned. This was the first of the "Special Projects," and as he himself states: "While ours was the first large organization of its kind, it surely will not be the last. For this reason alone, the story of the Manhattan Project is worth telling." In the current development of our complex weapon systems, of course, the vertical organization approach is standard; Polaris, for example, has its Special Projects Office of the Bureau of Naval Weapons. Those now concerned with the management of such programs will recognize themselves and their problems in this book and will find the reading of it a rewarding experience.

* * *

Thinking About the Unthinkable, by Herman Kahn, Horizon Press, New York, 1962.

The *Unthinkable* of the title is, of course, thermonuclear war which was the title of another book by the same author in 1960. Mr. Kahn's earlier book elicited extravagant and contradictory comments. Thomas C. Schelling, Professor of Economics at Harvard, called the author "the most exciting military strategist in the country," while James R. Newman, editor of *World of Mathematics*, said: ". . . no one could write like this; no one could think like this . . .," and he called *On Thermonuclear War* an "evil and tenebrous book, with its loose-lipped pieties and its hayfoot-strawfoot logic . . . its bloodthirsty irrationality." Mr. Kahn's current book re-presents much of the same sort of thing that was presented in *On Thermonuclear War*, and it is doubtful that his new defenses of his concepts or the methods of analysis will convince the doubters—or disappoint his supporters. His thesis is that the possibility of thermonuclear war must be faced boldly and that such a war must be studied intensely—how to prevent it, what to do if it occurs. He tends, however, to ignore political factors, and, quite obviously, the use of what he calls "doomsday machines" could invalidate most of his theories. Because of the unknowns and the intangibles, war is an art, not a science, and perhaps one of the major weaknesses of this book is the tendency of the author to deal with war as with a mathematical equation. He has, however, focused attention upon the problems of thermonuclear war, and his conclusions are provocative and interesting even if they must be balanced by a consideration of political factors, the intangibles of human nature and the lessons of experience.

* * *

Strike in the West, by James Daniel and John G. Hubbell, Holt, Rinehart and Winston, New York, 1963.

The title of this timely book on the actions of the United States in regard to Cuba is derived from the Soviet policy of fixing the attention of the world on affairs in the East, i.e., Berlin, while at the same time preparing to strike in the West. The authors present for the first time a detailed account of the recent missile crisis that brought the world to the brink of war. The facts which are marshalled here may not be new to the reader, but the arrangement constitutes a chilling pattern that may cause wonder and alarm at the inability of the government, served by a world-wide intelligence-gathering system, to interpret correctly the growing mass of evidence of Soviet activities. Attention is given to the confusing lack of agreement on what constitutes offensive as opposed to defensive weapons. There is also an interesting reconstruction of White House meetings on how to meet the threat—by an invasion which, it was estimated, might cost 5000 lives; by a surprise air attack to eliminate the missile bases; or by a blockade which might be followed, if necessary, by more drastic action. For some of us here, obviously, this book will have a heightened interest.

Soviet Communications Journals as Sources of Intelligence

BY [redacted]

(b)(3)-P.L. 86-36

~~Secret Kimbo~~

The collection of foreign intelligence is accomplished in a variety of ways, not all of them mysterious.

—Allen Dulles, *The Craft of Intelligence*

"Sputnik will contain two transmitters, with frequencies of about 20 and 40 mc; radiated power will be about one watt. . . . Sputnik's signals will be c.w. dashes .05 to 0.7 second long. The transmitters will operate alternately, the mark of one corresponding to the space of the other."

This announcement, published in the June 1957 issue of the Soviet magazine *Radio,* was intended to acquaint Russian radio amateurs with the signal characteristics of Sputnik I so that they would be prepared to monitor the signals once the satellite was launched. The next two issues of *Radio* contained additional details of Sputnik's transmissions.

If we Americans had been reading *Radio* as carefully as the Russians were, we might have been better prepared to receive Sputnik's signals when it was launched a few months later. We would have known, for example, that the transmissions were to be on 20 and 40 mc instead of on 108 mc, as had been agreed upon in the IGY satellite program. Our failure to act upon—perhaps even to notice—the announced change in frequencies meant [redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

The example of Sputnik illustrates rather dramatically the value of Soviet technical journals as sources of intelligence. If we learned nothing else from Sputnik, we learned that what the Russians write in their technical publications is worth reading. If these journals were little read in the West before Sputnik, today they are read widely and carefully.

Using [redacted] as an example, let's see how useful Soviet communications journals are as sources of intelligence at NSA.

(b)(3)-P.L. 86-36

[redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

As these examples show, the "open sources" are particularly good for providing information [redacted]

(b)(3)-P.L. 86-36

[redacted]

Which are the good sources? [redacted]

Pravda and *Izvestiya* sometimes provide miscellaneous items of interest—[redacted] Except for a few old issues which are available, copies of this magazine unfortunately seem to be almost impossible for foreigners in the USSR to buy, borrow or steal.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

The Russians are prolific publishers of books and pamphlets which are sold widely at very low cost. While some of those in the communications-electronics field are written in a popular science vein, there are also serious works, and these are worth looking at. Those which we have used range from booklets [redacted]

As guides to what the Russians are publishing in our field, we use the various periodical indexes and book catalogs published in both English and Russian. [redacted]

A considerable amount of Soviet scientific and technical information is now available in translation. In the communications field, complete translations of the magazine *Elektrosvyaz'*, *Radiotekhnika*, *Radiotekhnika i Elektronika*, and *Vestnik Svyazi* are available in

English. Individual articles, pamphlets and books are also translated by various government and private organizations, notably by the Joint Publications Research Service. Many of the news items from *Pravda* and *Izvestiya* are published in CIA's daily *Foreign Broadcast Information Service* reports. Abstracts of articles from Russian electronics journals are prepared by an Air Force unit at the Library of Congress. Others are published by commercial translation services in digests such as *Electronics Express*.

Finally, how reliable are the Russian sources? Since they are written by communicators and are intended to impart information to other communicators, there seems to be little reason for willful distortion. If allowance is made for a small "bragging factor," the sources can generally be considered reliable. We consider them not only reliable but valuable.

Something May Rub Off!

F. W. LEWIS

~~Confidential~~

As an itinerant journeyman cryptanalyst, I have spent a fair portion of my Agency life visiting operating sections for varying periods of time—days, weeks, or months. These house-guest tours have usually been occasioned by the appearance of a new and possibly challenging (but hopefully yielding) problem or an unexplained twist to an old problem. They were made with my host's approval—occasionally even on invitation—so it would scarcely display good manners to impute to them any lack of awareness of the need for improved technical procedures and higher standards of scientific approach. But increasingly I have become conscious of a possible blind spot in our cryptanalytic vision which may seriously hamper the continuing growth of within-section cryptanalytic competence.

The problem, simply stated, is "How does the working cryppie, in sections where most technical challenges are of the same kind and where there is little opportunity for original analysis of widely varying systems, acquire the knowledge, experience, and skill necessary for the expeditious handling of a cryptographic innovation?"

An equally serious (though possibly less frightening) poser might be "Have we any assurance that middle-level analysts are not muddling through, laboriously bludgeoning answers out of a problem with outmoded techniques?"

The answer to these questions may well lie in a more judicious application of an old educative stand-by—the tutorial method of learning.

In the leaner years of our intelligence effort (from a standpoint of resources—personnel and tools) it was taken for granted that the best training for the novice was as an apprentice to a more experienced analyst who was willing and eager to share his crypt knowledge, and even the fairly well-trained analyst could benefit from working at the elbow of a proven master of the science. This implies a certain amount of rapport between the various levels of skills and experience, and a willingness to spend a few moments in explanation, theoretical analysis, and technical shop-talk.

However, with the gradual—and quite logical and proper—change in the character of the Agency from a small, more personalized, and highly motivated fraternity to a large organization embracing many different specialized skills and semi-autonomous full-scale activities, it is quite natural that attendant problems associated with communication, training, and technical breadth should crop up.

Among the many understandable reasons for the appearance of well-appreciated but difficult-to-solve dilemmas, one might include:

(1) The requirement for large numbers of less professionally-trained workers in jobs calling for specific rather than broad skills.

(2) The magnitude of problems involving so many different technical and management aspects that few people are in position to appreciate more than selected portions.

(3) The security constraints which necessitate much tighter controls, compartmentation and established need-to-know.

(4) The fantastically powerful tools available, the complexity of which demands a team approach rather than single-handed effort. (Combined with item 2 above and the changing character of so many problems, this relegates the "Black Chamber" romantic concept of individual victory to a historical period somewhere between the Black Knight and Sgt. York.)

Among the less understandable reasons for this present alarum and excursion, I would list several evils which I sincerely trust are only indicative rather than wide-spread:

(1) The lack of technical understanding and appreciation on the part of certain middle-level supervisors. Perhaps this is an attendant evil of the healthy desire to give all established personnel equal opportunity to grab the next rung on the ladder, but too narrow a field of personal technical achievement may place a very competent technician in one restricted field in the awkward position of making decisions affecting problems completely beyond his understanding.

(2) An overly insistent attitude on the part of some section heads that they must appear to be self-sufficient, even when help is obviously needed. The striving for an intra-mural technical competence is laudable; the pettiness that sweeps incompetence under the rug rather than admit a need for assistance is not. This has reached nadir when section analysts are called on the carpet for seeking the advice of staff specialists, thereby making the section "look bad."

(3) A total lack of appreciation on the part of a few analysts of the new and powerful tools at our disposal. When RYE suggests only a beverage to technicians who have been pushing a pencil for ten or more years and when STETHOSCOPE is only something that needs warming before application, our methods salemen have obviously not been making the correct rounds.

(4) The tendency on the part of some consulting analysts, detailed temporarily to a section, to bury themselves in a corner, and independently and individualistically work out the answer to a knotty problem before emulating the Arab tent-folders. Bailing out a section is not enough; the visiting analyst has failed in a major part of his mission if the problem had been alleviated, but the human factors have been ignored.

It is with regard to the last of these complaints that I make my strongest plea. While we as individuals perhaps cannot always fully appreciate the more subtle problems of administration within the Agency's unique confines of mission and security, we as technicians can make the most of our technical consciences to do the best job possible according to the highest professional standards. This implies a dedication to the principles of professional integrity and scientific achievement, with full regard for the continual growth of the technical competence of the Agency to handle its collective problems, as well as concern for the growth of individual technicans.

The mechanics of fostering a wider technical understanding and competency in an informal way can be kept rather simple if certain assumptions are made. These assumptions involve:

(1) A climate of professionalism that can make the science of cryptology a stimulating challenge to the majority of analysts;

(2) A recognition of the fact that a broad spectrum exsits, which embraces varying degree of skills within levels of technical proficiency. As in many other professions, there are apprentices, journeyman technicians, and master craftsmen, with a logical progression through the various levels contingent on talent, training, and technical application—plus time and opportunity.

The precepts I would recommend to be followed as personal guidelines (within the natural boundaries of administrative and security procedures prescribed) are:

(1) *Learn the trade.*—The inquiring mind—hopefully never quite satisfied in the search for new ideas, new techniques, new knowledge—can take advantage of the experience of other professionals by a receptive attitude towards formal training courses, lectures, literature and personal contacts with more experienced technicians. Admittedly, an important factor in this is opportunity, but few of us take advantage of a fraction of the chances that do present themselves.

(2) *Learn the tools.*—Many cryptanalytic techniques have been revolutionized within the last decade, due to the impact of large-scale, high-speed computers. Theoretical attacks of yesterday are routine procedures now, and both diagnostic procedures and exploitation methods have vastly different potential applications. However, the gulf between raw data and finished product may yawn even wider if the human *interpretive* element is neglected in a blind devotion to the principle of mechanization. We must first know what to do and how to do it—which diagnostic technique, which machine approach promises the best opportunity. Then, in many cases where a machine can only go so far in presenting facts for consideration, the real problem of analysis begins. The more conservative voices who insist that no machine has ever "solved" a problem may be quite right—a silver-platterful of important raw ingredients does not constitute the dainty dish our customers might be expecting. Whether it be cryptanalytic phenomena, the potentials of a traffic analysis exploitation, or tid-bits of semi-processed intelligence, someone

must decide what the stuff means and what it implies as our next step. Finally, the use of optimum procedures for continued exploitation demands knowledge of perhaps entirely different techniques and machines.

Oftentimes tools are left unhoned merely because certain experts feel they don't need them. For example, experienced linguists have the tendency to consider language frequency counts, pattern lists, and stereotypes as implements too primitive for their professional status. The result is that a willing experienced non-linguist may be frustrated in a basic attack, since relative weights are presumably applied intuitively. ("I'll recognize it when I see it!") We know of established sections where a valid frequency count has never been made on individual letters of plaintext, let alone the more sophisticated statistical tabulations of digraphs, word endings, and the like.

(3) *Read—and write.*—The amount of available written information concerning historical crypt systems, the cryptography and cryptanalysis of the major enciphering machines, and the theoretical approach to almost any potential problem is admittedly overwhelming. But judicious use of background material, historical documents, library information and text-book approaches may save months of trial and error. A bright and determined eager-beaver can usually figure out for himself an approach that has long been recognized as applicable. But wheels do not have to be continually reinvented.

As a corollary, one should feel compelled to economize on another person's time and effort by recording progress (or lack thereof) on any non-trivial project. How often we see the same problem tackled over and over by succeeding waves of analysts, each time starting from scratch, with the same elementary statistics forthcoming and the same preliminary deductions independently worked out. Building on a predecessor's groundwork is entirely valid, provided that proper sampling and spot-checking justify confidence in the accuracy of the work and logic of first reasoning. Properly labeled work sheets, intelligible notes, technical devices, and interim reports—each has its value when you (or another analyst) may venture to pick up the thread at a later date.

It is unfortunately true that need-to-know and other security restrictions inhibit the rather wide inter-section exchange of progress reports and technical notes that made for vicarious experience in the older days; but within authorized limits there is still opportunity to learn typical problem approaches and typical procedures in the not unrealistic hope that one may be able to use the same trick tomorrow on a problem within his own bailiwick. Even comparatively trivial desk aids may be worth mentioning to others; for example, a clever little plastic "make-your-own-grille" device I saw the other day for the first time. [redacted]

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

(4) *Give out as well as take in.*—This could be paraphrased as "Strive to be a good teacher as well as an apt pupil." Almost every technician, regardless of his rank within the hierarchy of talent and experience, has at some time acquired a special knowledge, some useful technique or a helpful suggestion that would make life simpler for the poor soul at the

next desk. At the risk of seeming to put into the script a stage set for one loud continuous scene of conflicting dialogue, I say "talk it up a little." With all due respect to the conservative supervisor who likes to survey a nice quiet roomful of deeply concentrating, strong-but-silent types, I feel that there is room for the desk-level give-and-take technical discussion, the informal technical "bull-session" (or what the British refer to as tea-parties), and the occasional spontaneous black-board talk on an immediate problem, a noteworthy phenomenon, or an exciting development Naturally, such activities should be kept within reasonable bounds, both as to time and place. (Perhaps certain areas should be reserved for more rough-and-tumble competitive mental gymnastics, while other spots are off-limits to anyone other than the "Quiet-Man At Work" type.)

The need for the closely-buttoned lip one sees in the Security posters (and I hasten to agree with the intent and spirit of such) does not extend to technical exchange of ideas relating to a specific problem within the confines of the section having proper jurisdiction over it.

In summary, let's not degrade the professional approach. We must be prepared to be sponges in the matter of absorbing ideas and techniques, and well-controlled faucets when the next-door neighbor's well is in danger of running dry. Above all, we must not be too proud to listen or too hesitant to speak up if something of apparent value is gettable or giveable. For cryptanalytic experience can be shared, and the time, effort, and patience of the more experienced analyst could not be better spent than on insuring our Agency's future cryptanalytic know-how through sharing knowledge with a competent and willing but less experienced apprentice. More positively stated than in the title of this essay—something is *bound* to rub off.

Time Is - Time Was - Time Is Past
Computers for Intelligence

BY HOWARD H. CAMPAIGNE

Unclassified

The "Intelligence" of the sub-title does not mean "military information," which it could very well at a conference* like this, but means rather "adaptive behavior," or "imagination," or "pattern recognition." Frankly, I do not have a single definition for what I mean, but a recurring idea (See Bibliography) has been that some day a machine might be made which exhibited intelligence. Roger Bacon was the first to succeed, it was said, but his machine refused to discuss trivialities with man and then destroyed itself in frustration at man's inability to communicate with it. The story of Roger Bacon is that he succeeded in building an artificial intelligence, probably in the year 1277 or just before that, for that was the year in which he was arrested and imprisoned, charged with "innovations." It was a defense project, the ultimate objective being to build a wall of brass around England. His intelligence was housed in an artificial head. It took him 7 years to build it—about right for a defense project. When it was done, he spent 60 days debugging, mostly overtime. That sounds familiar. This debugging stretch was ended by the irresistible need for sleep, so he left his assistant in charge. That clown could hardly wait for Friar Bacon to fall asleep in order to push the start button. The head said "Time is," and lit the halt light. Some clownish talk and another push on the button elicited "Time was." More irrelevant comments and a button push caused the shout "Time is past," and the machine smashed itself on the floor. That was the end of the project. Clearly the head was about to say that to get support they needed the term a "real time system," but it could not make itself understood. This scene of acute frustration has typified artificial intelligence ever since.

The report on this was written by Robert Greene in 1588, 311 years later, almost a record delay for a progress report. It was typed in 1592 and released in 1630. A bad precedent.

If we are to have a demonstration of intelligence by a machine, we must agree in advance on what constiutes an adequate demonstration. I have talked to some of my colleagues about this, and I despair of ever getting any agreement. By and large there is some

* Read before the MIL-E-CON 8, 16 Sept 1964.

consensus that by an intelligent machine we mean one which exhibits human behavior of some kind. Turing[1] reduced this to a contest with teleprinters (a weapon which computers can use readily) and defined intelligence as the ability to imitate a man. Kelly and Selfridge[2] suggested an even simpler game. But beyond this there is no agreement. Some of my friends would be satisfied that a machine was intelligent if it could outperform some human being. But there are human beings–present company excepted–whose performance is miserably low, and this standard may already have been met. Others, also my friends, would not admit intelligence in a machine unless it excelled all human beings. If it could do this, then who would be the judge?

If we are to demonstrate intelligence in a machine, we must decide what we mean. To do this we can start at either end; what can a machine do or what can a man do? The latter is not nearly as well understood as one would think. The abilities lumped together under the word "intelligence" are various and not ordinarily distinguished clearly one from another. Occasionally an "idiot savant" appears who demonstrates vividly that intelligence is composite. He can do arithmetic with great ease but is unable to comprehend social relations, or he has great skill in music but none in language, or exhibits some other such striking disparity in abilities. Finding what these abilities are is the unfinished job of the psychologist.

These two approaches are like digging a tunnel by starting at both ends, although in this case we know so little of the mountain that we don't know that these diggers are even going toward each other, let alone whether they will meet. And if, by accident, they should meet, we don't know of what use the tunnel will be!

To my mind, the more productive way is to start with the machine and find what limits its ability. Even if such a program has a negative result and shows that intelligence is not achievable by a machine and that man is able to do something of a higher type, it will be useful to know the boundaries. I do not expect this to be the result. I think that as we learn more of what machines can do and more about what is rational behavior by human beings the question will go away.

A useful analogy is the development of flying. For centuries men dreamed of imitating birds. DaVinci made drawings of linkages which would work a wing DaVinci wrote "A bird is an instrument working according to Mathematical law, which instrument it is

[1] Alan Turing, "Computing Machinery and Intelligence" *Mind*, 59, New Series 236, October 1950, pp. 433–460.

[2] J. L. Kelly, Jr., and O. G. Selfridge, "Sophistication in computers: a disagreement," *IRE Transactions on Information Theory*, 1962, IT–8, pp. 78–80

within the capacity of men to reproduce with all its movements." At that time arguments were advanced that "birds are supported by the hand of God" and "if He meant us to fly, God would have given us wings." In the end it was components unknown in nature, the propeller and the internal combustion engine, that opened the way to a solution. These components were developed by people more interested in what could be done with engines than they were in imitating birds. The Wright brothers' solution was not satisfactory to all concerned, and interest in ornithopters continued for a while, but now the question of how closely a man can imitate a bird is dormant.

Meszar[3] said "any mental process which can be adequately reproduced by automatic systems is not thinking." Since then we have had the following demonstrations: theorem proving by Gelernter, checkers playing by Samuel, music composition by Hiller and Isaacson, assembly line balancing by Tonge in 1961, designing motors by Gold in 1959, and freshman calculus by Slagle in 1961.

Minsky[4] has listed, as clearly as the muddled state of the art permits, operations which must be performable by any thinking machine. He describes these as search, pattern recognition, learning, planning, and induction. The order cited is that of increasing sophistication, that is to say, of decreasing understanding. There have been respectable demonstrations of each of these except the last, induction. Search has been implemented and written about by a great number of investigators; the simplest of the concepts, it still furnishes much discussion and is not to be disposed of in the near future.[5] Pattern recognition here means matching against a prototype; this is being done commercially as in the reading of checks written with magnetic ink, although the limitations on the technique are not well understood. Learning is here restricted to adaptive behavior, which in its simplest form can be easily demonstrated, but which titilates us in our limited ability to generalize; in its most general form it would solve all of our problems. If we equate adaptive behavior with learning and if we assume no limit on learning (why should it be limited?), then, as I. J. Good says, this is the last invention man will ever have to make. What Minsky calls "planning," I would call "reformulation." Demonstrations of this have been made by Newell, Shaw and Simon,[6]

[3] J. Meszar, "Switching Systems as Mechanized Brains," *Bell Telephone Record*, February 1953.

[4] Marvin Minsky, "Steps Toward Artificial Intelligence," *Proc IRE*, 49, 1961, pp. 8–30.

[5] For example, C. E. Shannon, "Programming a Computer to Play Chess," Philosophical Magazine, 7, 41, 1950, pp. 225-275.

[6] Alan Newell, J. C. Shaw and H. A. Simon, "Empirical explorations of the logic theory machine," *Proc WJCC*, 1957, pp. 218-230.

who show a way of finding pertinent intermediate goals. The last in his list is induction; this is the $64 question as we see it today; no demonstrations have been made that I know of. Another name for induction is jumping to conclusions.

Newell says "if ever a fully capable intelligent program is realized, it will be recognized by noting that it can get along without any programmer at all."[7]

Minsky says "Almost any problem can be converted into a problem of finding a chain between two terminal expressions in some formal system."[8]

Let me go over Minsky's list again, this time looking toward the directions in which these techniques, if we had them, would generalize. The problem of search, listed by Minsky as the first step in his program toward artificial intelligence, has great generality and has had many contributions from many sources. Hill climbing, the method of steepest descent, heuristic methods, all are attempts to find ways to exploit the structure of the space being searched. Basic as this technique is, it still may be of complete generality, for any solution can be stated in terms of a choice of paths. If one thinks of search as analogous to a man exploring territory, then the amount he can see at one time is the important parameter. Crossing the plains toward a distinctive peak in daylight is different from thrashing through the jungle in the dark.

The term "pattern recognition" could be interpreted to mean the perception of similarities in previously undigested data. In this broad sense it is very much like, perhaps equivalent to, induction. It was not used in this sense by Minsky. In the narrower sense of recognizing a resemblance to a prototype it still is powerful in categorizing concepts.

"Learning" too is often used more broadly than Minsky used it. A device which was adaptive in the broadest sense could accommodate to any situation, barring a catastrophe. The biological ecological system of evolution may be doing just this. The analogy between evolution and learning is a striking one but also painful because of the slow reaction of the first. Evolution is a blind search. The ecological system is searching in parallel, of course, but each species is trying to solve its own problems alone. If one thinks of the genetic possibilities as a space with as many dimensions as there are genes and

[7] M. C. Yovits, G. T. Jacobi, G. D. Goldstein, "Some problems of basic organization in problem-solving programs," *Self-organizing Systems*, Spartan Books, Baltimore, 1962.

[8] Marvin Minsky "Steps Toward Artificial Intelligence," *Proc IRE*, 49, 1961, pp. 8–30.

as many points on each axis as there are alleles, then each individual's heritage can be represented by a point in this space. In the case of a monosexual species (if there are any), each strain is making its own path. Bisexual species advance in a herd, each specimen being at a point in the genetic space A herd can split, of course, but the splitting is limited by the fact that each species is at a local maximum, or trap. When dislodged from its cul-de-sac, a species mutates fairly rapidly and generally toward what seems like conscious direction, uphill perhaps, a phenomenon noticed long ago by geneticists and called "orthogenesis."

By "planning" Minsky means the substitution of intermediate goals as means to an ultimate goal. This is akin to reformulation, if not the same, a step which I am sure is essential to human problem solving. Our experience in scientific research is that once a question has been properly put, the answer generally follows in short order. A researcher spends more effort wrestling with questions than he does with answers. Those questions which seem to be well put but for which no answer has yet been found are famous, such as the four colored map problem. This substitution of goals has been demonstrated by Newell, Simon and Shaw[9]. In the context of searching through a graph, it is easily seen that the intermediate goal is an island of great value. If one had a problem which required the determination of six parameters, each with forty possible values, then a blind search would be faced with four billion places to look. If a sub-goal can be found so that three parameters can be determined first and then the other three, we find that only 2 × 64,000 places need be searched, or 128,000. The existence of the sub-goal is worth a factor of 32,000. The existence of such goals depends on the structure of the problem, of course.

Induction is the reasoning from a part to the whole, the predicting of new events from past events. To do this predicting, one needs a model of the world, or of the relevant parts of the world. The construction of the mathematical model from a sample is the step we do not understand. It is jumping to a conclusion, which, up to now, machines do not do so well. The most formal kind of induction, mathematical induction, is a special case of deduction, an operation done very well and commonly by machines. Perhaps there is little difference between the two kinds of reasoning, and our fears of the unknown are not justified.

When I started this paper, I meant to work toward specifying a machine or computer useful in experiments on artificial intelligence. If we are going to experiment with thinking computers, what kind of

[9] Newell, Shaw and Simon, *op. cit.*

machines would we like? Software improvements are a necessity, but a number of other things suggest themselves.

One is speed. If our computer could explore our game of chess to the very end, then, of course, it would have insight; but this is impossible with chess and with many other problems, because of the tremendously ramified argument. Chess has been quoted as having 10^{120} positions, and if only a millionth of these were relevant and if they could be disposed of at a million a second, it would take 3×10^{100} years to exhaust them. So speed by itself will not do much; it will take software.

Another is parallelism. Selfridge[10] has described an organization resembling a situation room which has a big board on which the latest data is available to all, and which can be continually updated by each of a large number of demons: pandemonium. Such an organization might have advantages in learning. There is reason to think that the human brain may be a little like this, a committee of slow components. The programming of such an organization is almost unexplored.

An alternative is that of distributed logic, an assemblage of data-manipulating equipment, especially memory, each of which can do some of the essential processes such as sensing and combining Thus the logic, instead of being concentrated in the accumulator or control, would be everywhere. A content addressed memory is a kind of distributed logic; with this, one can do many complex operations, such as sorting, almost painlessly. Improvements in software have more to offer.

But a useful thinking machine must have flexible input-output, an effective interface with men. Like Bacon's head, if it cannot get through to us, it might as well not exist. And we too have our language problems and need to have the very best of aids in stating problems to the device and reorganizing the thinking of our machine. This is the area which needs most improvement, the easy interchange of information between man and machine.

Buchman also has characterized the various properties of an intelligent machine in a different but very clear way.[11] He says that such a machine must be adaptive, self-organizing, or learning. By "adaptive" he means stable in a changing environment; by "self-organizing" he means effective in a radically changing environment;

[10] Oliver Selfridge, "Pandemonium: A Paradigm for Learning," *Paper 3-4*, Teddington Symposium, November 1958.

[11] A. F. Buchman, "The Digital Computer in a Real-Time Control System, Part III," *Computer Design*. Vol. III, No. 5, May 1954, pp. 24–31.

and by "learning" he means increasingly effective in a stable environment.

I must comment on a statement I have seen that soon the chess champion will be a machine! This is fatuous. Bicycles are not used in the Olympic footraces; if they were, a cyclist would be world champion. When the rules of chess are amended to prohibit mechanical aids, that will be a clue that one of our subgoals is being approached.

May I suggest that Turing's test with the game of bridge might be effective? Played by teletype, it would be the task of each player to identify the machine among the three other players. Or if bridge is too much work to program, then a series of checkers games, where a man plays alternately with a champion and with Samuel's superlative checker program, the man's task being to name which is which. This could be implemented readily because Samuel's part is done.

If a thinking machine can be built, then it must be done; it is a matter of self-respect. Just as a man must be put on the moon, just as Mount Everest had to be climbed, just as the poles had to be visited, just as a flying machine had to be made no matter what the arguments against it, so a machine must be made which can think.

Taube has said " . . . The proper man-machine relation is one of complementation . . . "[12] I do not gain-say this; I agree. But the demonstration must be made nevertheless. Seashore's story illustrates the state of the art.

[12] Mortimer Taube, *Computers and Common Sense: The Myth of Thinking Machines*, Columbia University Press, 1961.

BIBLIOGRAPHY ON EXTENDING SCOPE OF COMPUTERS

S. Amarel, "On the Automatic Formation of a Computer Program which Represents a Theory," *Self Organizing Systems*, Spartan Books, Washington, D. C., 1962.

A. M. Andrew, "Learning Machines," Paper 3-6, Symposium on the Mechanization of Thought Processes, Teddington, England, November 1958.

James B. Angell, *The Need and Means for Self-Repairing Circuits*, Technical Report No. 4654-2, USAF Contract AF33(616)-7726, Stanford Electronics Laboratories.

Paul Armer, "Attitudes toward Intelligent Machines," *Datamation*, Vol. 9, No. 3, March 1963, pp. 34-38.

————, "Attitudes toward Intelligent Machines," RAND Corp., p 2114, 30 September 1960. (Extensive bibliography.)

J. A. Aseltine, A. R. Mancini, and C. W. Sarture, "Impulse-Response Self-Optimization as Compared with Other Criteria for Adaptive Systems," Presented at 4th Annual Instruments and Regulators Conference on Automatic Optimization, University of Delaware, 4 April 1958.

W. R. Ashby, *Design for a Brain*, John Wiley & Sons, Inc., New York, N. Y., 1952. (Chapman and Hall, London.)

————, "Design for a Brain," *Electronics Engineering*, 20, 1948, pp. 379-383.

————, "Computers and Decision Making," *New Scientist*, 7, 746, 24 March 1960.

————, "Design for an Intelligence Amplifier," *Automata Studies*, *Annals of Mathematical Studies*, No. 34, Princeton University Press, 1956, p. 215.

————, "What is an Intelligent Machine," *Proc. WJCC*, Vol. 19, May 1961, p. 275.

————, and J. Rignet, "The Avoidance of Over-Writing in Self-Organizing Systems," Technical Report No. 1, Burden Neurological Institute, Bristol, England.

M. L. Babcock *et al*, "Some Principles of Preorganization in Self-Organizing Systems," Electrical Engineering Research Laboratory Report No. 2, University of Illinois, 24 June 1960.

R. B. Banerji, "Computer Programs for the Generation of New Concepts from Old Ones," Case Institute of Technology. (Preprint)

H. B. Barlow, "Sensory Mechanisms, the Reduction of Redundancy, and Intelligence," Symposium on the Mechanization of Thought Processes, Teddington, England, November 1958.

B. L. Basore and W. D. Wood, *A Model for Communication with Learning*, Dikewood Corporation TN-1004-2, 31 May 1960.

A. Bernstein *et al*, "A Chess Playing Program for the IBM 704," *Proc. WJCC*, 1958, pp. 157-159.

A. Bernstein and M. deV. Roberts, "Computer vs. Chess Player," *Scientific American*, 198, June 1958, pp. 96-98.

"Bibliography on Biological and Artificial Intelligence," Jet Propulsion Laboratory, California Technical Literature Search No. 254 and Supplement.

W. W. Bledsoe and I. Browning, "Pattern Recognition and Reading By Machine," *EJCC*, Boston, December 1959, pp. 225 232.

R. R. Bush and F. Mosteller, *Stochastic Models for Learning*, John Wiley & Sons, Inc., New York, N. Y., 1955.

Silvio Ceccato, "La Machine qui Parle et qui Pense," *Congress International de Cybernetique*, Namur, 1956.

C. K. Chow, "An Optimum Character Recognition System using Decision Functions," *IRE Trans. on Electronic Computers*, Vol. EC6, December 1957, pp. 247–254.

W. A. Clark and B. G. Farley, "Generalization of Pattern Recognition in a Self-Organizing System," *Proc. WJCC*, 1955, pp. 86–91.

W. E. Dickinson, "A Character-Recognition Study," *IBM Research and Development*, Vol. 4, July 1960, pp. 335–348.

T. L. Dimond, "Devices for Reading Handwritten Characters," *Proc. EJCC*, Washington, D. C., December 1957, pp. 232–237.

G. P. Dineen, "Programming Pattern Recognition," *Proc. WJCC*, March 1955, pp. 94–100.

W. Doyle, "Recognition of Sloppy Hand-printed Characters," Lincoln Laboratory Group Report 54–12, December 1959.

T. G. Evans, *A Heuristic Program for Solving Geometric Analogy Problems*, unpublished Doctoral Disseration, MIT, 1963. (Also Spring *JCC*, 1964, pp. 327–338.)

B. G. Farley and W. A. Clarke, "Simulation of Self-Organizing Systems by Digital Computers," *Transactions on Information Theory, IRE PGIT*, 4, September 1954, pp. 76–84.

Edward A. Feigenbaum, "Artificial Intelligence Research," *IEEE Transactions*, Vol. IT–9, No. 4, October 1963, pp. 248–253.

E. Feigenbaum and J. Fedman, Eds., *Computers and Thought*, McGraw-Hill, N. Y., 1963.

Edward A. Feigenbaum and Gerbert A. Simon, "Forgetting in an Association Memory," *RAND* p–2311, 24 May 1961.

I. Flore and L. Grey, "Optimization of Reference Signals for Character Recognition Systems," *IRE Transactions on Electronic Computers*, Vol. EC–9, March 1960, pp. 54–61.

L. J. Fogel, "Toward Inductive Inference Automata," *Proc. 1962 International Conference of Information Processing*, Amsterdam, The Netherlands, 1963, pp. 395–400.

R. M. Friedberg, "A Learning Machine: Part I," *IBM Journal of R&D*, 2, No. 1, January 1958, pp. 2–13.

R. M. Friedberg, B. Dunham and J. H. North, "A Learning Machine: Part II" *IBM Journal of R&D*, 3, July 1959, pp. 282–287.

H. Gelernter and N. Rochester, "Intelligent Behavior in Problem-Solving Machines," *IBM Journal of R&D*, 2, 1958, pp. 336–345.

H. L. Gelernter, "Realization of a Geometry Theorem-Proving Machine," *Proc. Int. Conf. on Information Processing*, Paris, 1959.

————, "Theorem Proving by Machine," *IBM IR–00124*, August 1957.

A. Gill, "Minimum-scan Pattern Recognition," *IRE Transactions on Information Theory*, Vol. IT–5, June 1959, pp. 52–58.

————, "Possibilities for the Practical Utilization of Learning Processes," Paper 4–10, Symposium on Mechanization of Thought Processes, Teddington, November 1958.

P. C. Gilmore, "A program for the production of proofs for theorems derivable within the first order predicate calculus from axioms," Unesco, NS, ICIP, 1.6.14, International Conf. on Information Processing, Paris, June 1959.

————, "A Proof Method for Quantification Theory," *IBM Journal of R&D*, 4, 1960, pp. 28–35.

H. T. Glantz, "On the Recognition of Information with a Digital Computer," *JACM*, Vol. 4, April 1957, pp. 178–189.

B. Gold, "Machine Recognition of Hand-sent Morse Code," *IRE Transactions on Information Theory*, Vol. IT–5, March 1959, pp. 17–24.

I. J. Good, "The Subassembly Theory of Memory and Meaning and its Relevance to the Economical Construction of an Ultra-Intelligent Machine," May 1963.

S. Gom, "On the Mechanical Simulation of Learning and Habit Forming," *Information and Control*, 2, September 1959, pp. 226–259.

B. F. Green, A. Wolf, C. Chomsky, and K. Langhevy, "Baseball: an Automatic Question Answerer," *Proc. WJCC* 1961, pp. 219–224. ,

P. H. Greene, "An Approach to Computers that Perceive, Learn and Reason," *Proc. WJCC*, 1959, pp. 181–186.

————, "A Suggested Model for Information Representation in a Computer that Perceives, Learns and Reasons," *Proc. WJCC*, 1960, pp. 151–164.

————, "Networks for Pattern Perception," *Proc. National Electronics Conf.*, Vol. 15, October 1959, pp. 357–369.

E. C. Greenian and Y. M. Hill, "Considerations in the Design of Character Recognition Devices," *IRE National Convention Record*, 1957, pp. 119–126.

E. C. Greenian *et al*, "Design of Logic for Recognition of Printed Characters by Simulation," *IBM Journal of R&D*, Vol 1, January 1957, pp. 8–18.

R. L. Grimsdale *et al*, "A System for the Automatic Recognition of Patterns," *Proc. IEE*, 106, Pt. B, March 1959.

Fred Gruneberger, "Benchmarks in Artificial Intelligence," *Datamation*, October 1962, pp. 33–35.

George L. Haller, "Our State of Mind in 2012 A. D." *Proc. of IRE*, Vol. 50, No. 5, May 1962, pp. 624–627.

R. W. Hamming, "Intellectual Implication of the Computer Revolution," *Bell Telephone Laboratories*.

L. D. Hamon, "A Line-drawing Pattern-recognizer" *Proc. WJCC*, San Francisco, Calif., May 1960, pp. 351–364.

C. C. Heasly, "Some Communication Aspects of Character-sensing Systems," *Proc. WJCC*, San Francisco, Calif., May 1959, pp. 176–180.

W. H. Highleyman and L. A. Kamentsky, "Comments on a Character Recognition Method of Bledsoe and Browning," *IRE Transactions on Electronic Computers*, EC9, June 1960, p. 263.

M. E. Hoff, Jr., "Learning Phenomena in Networks of Adaptive Switching Circuits," Technical Report No. SEL–62–090, Stanford Electronics Labs., July 1962.

Aiko M. Hormann, "Programs for Machine Learning," TM–669/000/01 SDC 29 May 1962.

E. B. Hunt, *Concept Formation: An Information Processing Problem*, John Wiley & Sons, Inc., New York, 1962.

F. H. Jean, *Generation and Testing of Hypotheses*, Dikewood Corporation, FR–1021, Contract AF30(602)–2514 for Rome Air Development Center, 29 May 1962.

L. A. Kamentsky, "Pattern and Character Recognition Systems—Picture Processing by Nets of Neuron-like Elements," *Proc. WJCC*, San Francisco, May 1959, pp. 304–309.

J. L. Kelly, Jr., and O. G. Selfridge, "Sophistication in Computers: a Disagreement," *IRE Transactions on Information Theory*, IT–8, 1962, pp. 78–80.

T. Killren, R. L. Grimsdale, and F. H. Summer, *Experiments in Machine Learning and Thinking*, UNESCO/NS/1C1PJ.6.15, 1959.

R. A. Kirsch, C. Ray, L. Cahn, and G. H. Urban, "Experiments in Processing Pictorial Information with a Digital Computer," *Proc. EJCC, Proc. IRE.*, December 1957, pp. 221–229.

J. Kister, P. Stein, S. Ulam, W. Welden and M. Wells, "Experiments in Chess," *JACM.*, April 1957.

S. Kuroda, "An Investigation on the Logical Structure of Mathematics (XIII)—A Method of Programming of Proofs in Mathematics for Electronic Computing Machines," *Nagoya Mathematical Journal*, 16, 1960, pp. 145–203.

P. A. Lachenbruch, A. J. Slevenske and A. C. Marchese, "Artificial Intelligence—A Summary of Current Research & Development," American Institute for Research, Los Angeles, No. AIR–C63–2/62–TR, 1962.

J. C. R. Licklider, "Interactions Between Artificial Intelligence, Military Intelligence and Command and Control," preprints 1st Congress of the Information System Sciences, MITRE Corp., Bedford, Mass., 1962.

D. M. MacKay, "Mindlike Behaviour in Artefacts," *British Journal for one Philosophy of Science*, II, 1951, pp. 105–121.

Carl Maltz, "A Measure of the Significance of Pattern Features for Use as an Aid in the Design of Recognition Systems," Report 62–68, University of California, Los Angeles, December 1962.

T. Marrill and D. M. Green, "Statistical Recognition Functions and the Design of Pattern Recognizers," *IRE Transactions on Electronic Computers*, Vol. EC–9, No. 4, December 1960, pp. 472–477.

Henrik H. Martens, "Two Notes on Machine 'Learning,'" *Information and Control*, 2, 1959, pp. 364–379.

R. L. Mattson, "A Self-organizing Binary System," *Proc. EJCC*, 1959, pp. 212–217.

J. McCarthy, "Programs with Common Sense," *Mechanisation of Thought Processes*, Vol. I, National Physical Laboratory Symposium No. 10, Her Majesty's Stationery Office, 1959, pp. 75–84.

Warren S. McCuloch, "The Brain as a Computing Machine," *Electronics Engineering*, 69, 1949, p. 492.

J. Mesyar, "Switching Systems as Mechanized Brains," *Bell Telephone Laboratories Record*, February 1953.

Margaret Milligan, "Machines are Smarter Than I Am!" *Data Processing Digest*, October 1959.

O. N. Minot, "Automatic Devices for Recognition of Visible Two-dimensional Patterns; A Survey of the Field," US Naval Electronics Laboratory Technical Memo. 364, San Diego, June 1959.

M. L. Minsky, Appendix to "Steps Toward Artificial Intelligence," preprints, 1st Congress of the Information System Sciences, MITRE, 1962.

————, "A Selected Descriptor-Indexed Bibliography to the Literature on Artificial Intelligence," *IRE Transactions on Human Factors in Electronics*, Vol. HFE–2, No. 1, March 1961, pp. 39–56.

———, "Heuristic Aspects of the Artificial Intelligence Problem," Lincoln Laboratory Report 34-55, December 1956; ASTIA Doc. No. 236885, December 1956.

———, "Learning Systems and Artificial Intelligence." *Applications of Logic to Advanced Digital Computer Programming*, University of Michigan, Coll. of Eng., Summer Session, 1957.

———, "Some Methods of Artificial Intelligence and Heuristic Programming," *Proc. Symposium on the Mechanization of Thought Processes*, NPL Teddington, November 1958.

———, "Steps Toward Artificial Intelligence," *Proc. IRE* 49, January 1961, pp. 8–30.

———, and O. G. Selfridge, "Learning in Random Nets," *Fourth London Symposium on Information Theory.*

E. F. Moore, "On the Shortest Path Through a Maze," *Proc. International Symposium on the Theory of Switching*, Harvard, 1959.

G. A. Morton, "Machines with Imagination," *Proc. IRE*, Vol. 50, No. 5, May 1962, p. 611.

O. H. Mowrer, *Learning Theory and the Symbolic Processes*, John Wiley & Sons, Inc., New York, 1960.

Allen Newell, "Lectures on Heuristic Programs," *Engineering Summer Conferences, Summer Series*, Ann Arbor, Michigan, 1957.

———, "On Programming a Highly Parallel Machine to be an Intelligent Technician," *Proc. WJCC*, Paper 9.3, May 1960, pp. 267–282.

———, "The Chess Machine; An Example of Dealing with a Complex Task by Adaptation," *Proc. WJCC*, March 1955.

——— and H. A. Simon, "A Program that Simulates Human Thought," *Lernende Automaten*, H. Billing, Ed., Oldenbourg, Munich, 1961.

——— and H. A. Simon, "Computer Simulation of Human Thought," *Science*, Vol. 134, 22 December 1961, p. 2011.

———, J. C. Shaw, and H. A. Simon, "A General Problem-solving Program for a Computer," *Computers and Automation*, 8, 1959, pp. 10–17.

———, J. C. Shaw, and H. A. Simon, "A Variety of Intelligent Learning in a General Problem Solver," *Self-Organizing Systems*, M. C. Yovits and S. Cameron (Eds.), Pergamon Press, London, 1960, pp. 153–189.

———, J. C. Shaw, and H. A. Simon, "Chess-Playing Programs and the Problem of Complexity," *IBM Journal of R&D.*, 2, October 1958, pp. 320–335.

———, J. C. Shaw, and H. A. Simon, "Problem Solving in Humans and Computers," *RAND Corp.*, P-987, 7 December 1956.

———, J. C. Shaw, and H. A. Simon, *Report on a General Problem-Solving Program*, UNESCO/NS/1C1P/1.6.8; *Proc. International Conference on Information Processing*, Paris, pp. 256–264.

J. D. North, "The National Behavior of Mechanically Extended Man" Boulton Paul Aircraft Ltd., Wolverhampton, England, September 1954.

A. G. Oettinger, "Programming a Digital Computer to Learn," *Phil Mag.*, Vol. 43, December 1952, pp. 1243–1263.

———, "Simple Learning by a Digital Computer," *IRE Proceedings of the Association for Computing Machinery*, Toronto, Ontario, September 1952.

Proceedings of the Symposium on Mechanization of Thought Processes, H. M. Stationery Office, London, 1959.

W. C. Ridgway III, "An Adaptive Logic System with Generalizing Properties," Technical Report No. SEL-62-040, Stanford Electronics Labs., April, 1962.

P. I. Richards, "On Game Learning Machines," *Scientific Monthly*, 74, 4, 1952, pp. 201–205.

L. G. Roberts, "Pattern Recognition with an Adaptive Network," *IRE International Convention Record*, Pt. 2., 1960, pp. 66–70.

A. Samuel, "Appendix: Game of Checkers Played by Mr. R. W. Nealy vs Samuel Checker Playing Program," *Computers and Thought*, Feigenbaum & Feldman, 1963.

————, "Some Studies in Machine Learning, Using the Game of Checkers," *IBM Journal of R&D*, No. 3, July 1959, pp. 210–229.

O. G. Selfridge, "Pandemonium: A Paradigm for Learning," Papers 3–4, Symposium on the Mechanization of Thought Processes, Teddington, England, November 1958.

————, "Pattern Recognition and Modern Computers," *Proc. WJCC*, March 1955, pp. 91–93.

————, and G. P. Dinneen, "Programming Pattern Recognition," *Proc. WJCC*, March 1955.

————, and U. Neisser, "Pattern Recognition by Machine," *Scientific American*, 203, August 1960, pp. 60–68.

C. E. Shannon, "Game-playing Machines," *Journal of the Franklin Institute*, 206, December 1955, pp. 447–453.

————, "Programming a Computer to Play Chess," *Phil. Mag.* 7, 41, March 1950, pp. 256–275.

H. Sherman, "A Quasi-Topological Method for Recognition of Line Patterns," Unesco, NS, 1C1P, H. L. 5, International Conference on Information Processing, Paris, June 1959.

R. F. Simmons, "Syntex: Toward Computer Synthesis of Human Language Behavior," *Computer Applications in the Behavioral Sciences*, H. Barko Ed., Prentice-Hall, Inc., Englewood Cliffs, N. J., 1962.

Herbert A. Simon, "The Heuristic Compiler," *RAND*, Santa Monica, RM-3588 PR.

————, "Prediction and Hindsight as Confirmatory Evidence," *Phil. of Science*, 22, 1953, pp. 227–230.

————, and Allen Newell, "Computer Simulation of Human Thinking and Problem Solving," *Datamation*, 7 June 1961, pp. 18–20.

N. Sluckin, *Minds and Machines*, Penguin.

R. J. Solomonoff, "An Inductive Interference Machine," *IRE National Convention Record*, Pt. 2, 5, 1957, pp. 56–62.

————, "A Preliminary Report on a General Theory of Inductive Inference," Zator Technical Bulletin, v-131, ZTB-138, February 1960.

————, "The Mechanization of Linguistic Learning," *Zator Technical Bulletin*, No. 125, September 1958.

S. D. Steams, "A Method for the Design of Pattern Recognition Logic," *IRE Transactions on Electronic Computers*, Vol. EC-9, March 1960, pp. 48–53.

Mary Elizabeth Stevens, *Abstract Shape Recognition by Machine*, AFIPS 20, *Proc. EJCC*, 1961, Washington, D. C.

Donald N. Streeter, and Kumpati S. Narenda, *A Self-organizing Control System Based on Correlation Techniques and Selective Reinforcement*, Technical Report

No. 359, Craft Laboratory, Harvard, ONR Contract Nonr1866(16), NR–372–012, 20 July 1962.

D. L. Szekely, "On Basic Aspects of the Concept Transforming Machine," *Cybernetica*, Vol. 4, No. 2, 1961.

M. Taube, *Computers and Common Sense, The Myth of Thinking Machines*, Columbia University Press, 1961.

W. K. Taylor, "Pattern Recognition by Means of Automatic Analog Equipment," *Proc. IEE*, Vol. 106, Pt. B, March 1959.

————, "Electrical Simulation of Some Nervous System Functional Activities," *Information Theory*, C. Cherry Ed., Butterworth Scientific Publications, London, 1956.

W. H. Thorpe, "The Concepts of Learning and their Relation to Those of Instinct," Symposium of the Society for Experimental Biology, IV, p. 387.

J. H. Troll, "The Thinking of Men and Machines," *Atlantic Monthly*, July 1954.

A. M. Turing, "Can a Machine Think," *World of Mathematics*, James R. Newman, Ed., Simon and Schuster, 1956, Vol. 4, p. 2109.

————, "Computing Machinery and Intelligence," *World of Mathematics* Vol. 4, p. 2099; *Mind*, 59, October 1950, pp. 433–460.

L. Uhr, "Latest Methods for Conception and Education of Intelligent Machines," *Behavioral Science*, 4, 1959, pp. 248–251.

————, "Intelligence in Computing Machines; the Psychology of Perception in People and in Machines," *Behavioral Science*, 5, 1960, pp. 177–182.

S. H. Unger, "Pattern Detection and Recognition," *Proc. IRE*, 47, October 1959, pp. 1737–1752.

A. M. Uttley, "Imitation of Pattern Recognition and Trial-and-error Learning in a Conditional Probability Computer," *Rev. Mod. Phys.*, Vol. 31, April 1959, pp. 546–548.

B. Widrow and M. E. Hoff, "Adaptive Switching Circuits," Standard Electronics Laboratory, Stanford, Technical Report No. 1553-1, June 1960.

J. D. Williams, "Toward Intelligent Machines," *RAND Corporation P-2170*, 29 December 1960.

M. T. Yovitts and S. Cameron, *Self-Organizing Systems*, Pergamon Press, New York, 1960.