VII - 26 - X

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

HANDLING INSTRUCTIONS

1. This publication consists of covers and numbered pages 1 to 101 inclusive. Verify presence of each page upon receipt.

2. Formal authorization for access to SECRET material is required for personnel to have access to this publication.

3. This publication will not be released outside government channels without approval of the Director, National Security Agency.

4. Extracts from this publication may be made for classroom or individual instruction purposes only. Such extracts will be classified SECRET NOFORN and accounted for locally until destroyed.

5. This publication will not be carried in aircraft for use therein.

NATIONAL SECURITY INFORMATION
Unauthorized Disclosure Subject to Criminal Sanctions

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755

Revised July 1973

INTRODUCTION

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

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

RECORD OF AMENDMENTS

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

RECORD OF PAGE CHECKS

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

RECORD OF PAGE CHECKS

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

Subject
FIRST LE
SECOND
THIRD I
FOURTI
FIFTH
SIXTH
SEVEN
EIGHT
NINTI
TENT

TABLE OF CONTENTS

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

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

First, you'll note I said the opposition can do these things *if* he can intercept our communications. Let me first give you some facts about that supposition. You've all seen the security caveats asserting that "the enemy is listening", "the walls have ears", and the like. One of my irreverent friends, knowing where I work, insists on referring to me as "an electronic spy", and popular paperback literature is full of lurid stories about code-breakers and thieves in the night careening to Budapest on the Orient Express with stolen ciphers tattooed somewhere unmentionable. What is the actual situation?

[redacted] their collection facilities include large land based sites, mobile platforms (air and sea), and satellite surveillance; and that they have an extensive covert collection operation. All in all, a truly formidable opponent. So the first "if" underlying our argument for the need for COMSEC (Communications Security) is more than a postulate—a deliberate, large, competent force has been identified whose mission is the exploitation of U.S. communications through their interception and analysis.

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

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

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

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

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

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

Those of you who are cryptanalysts will find yourselves in an environment that is necessarily cautious, conservative, and with security *per se* a truly paramount consideration. This, I assert, is *healthy* because you, a mere handful, are tasked with outthinking an opposing analytic force of perhaps 100 times your number who are just as dedicated to finding flaws in these systems as you

must be to assuring none slipped by. But do not lose sight of the real world where your ultimate product must be used, and beware of security features so intricate, elaborate, complex, difficult, and expensive that our customers throw up their hands and keep on communicating in the clear—you have to judge not only the abstract probabilities of success of a given attack, but the likelihood that the opposition will be willing to commit his finite resources to it.

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

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

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

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

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

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

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

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

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

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

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

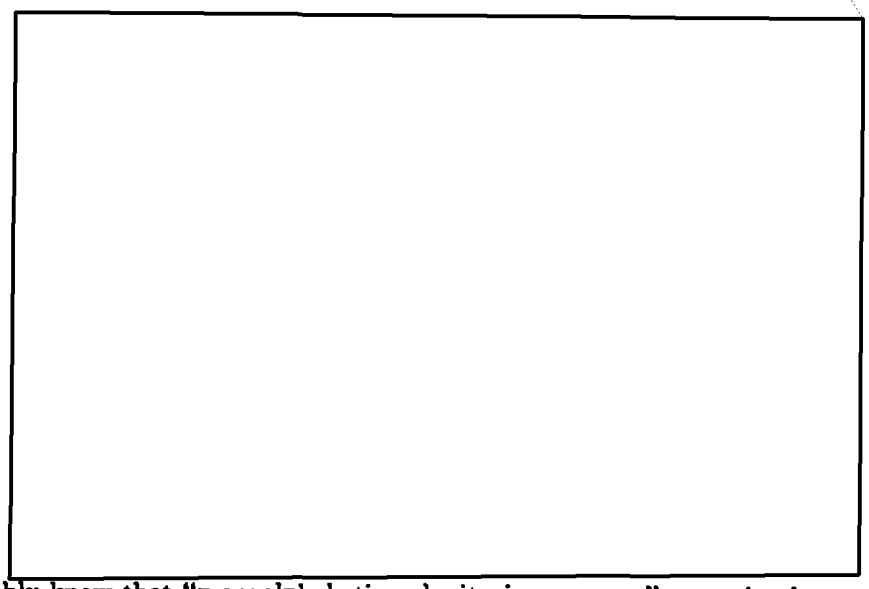
BRIGADE	ABT
COORDINATE(S)	AXQ
DIRECT ARTILLERY FIRE AT___	CDL
ENGAGE ENEMY AT	GGP
------	HLD
------	JMB

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

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

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

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



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

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

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

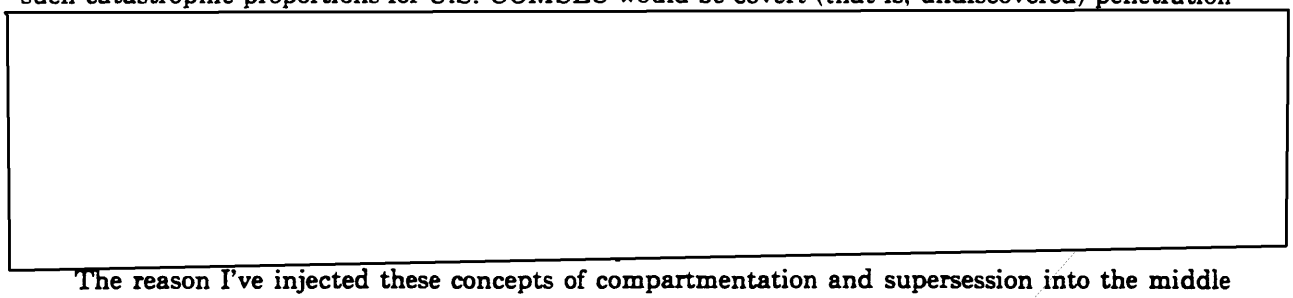
SUPERSESSION is simply the replacement of a code or other keying material from time to time with new material. Most keys and codes are replaced each 24 hours; a few codes are replaced as frequently as each six hours; a few others remain effective for three days or more. We have these differing supersession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

quire replacement as often. The regular replacement rate of material each six hours or 24 hours or three days or what have you is called the "normal supersession rate" of the material in question. "Emergency supersession" is the term used when material is replaced prematurely because it may have been physically lost.

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

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

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



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

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

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

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

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

. . . . . .
etc.

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

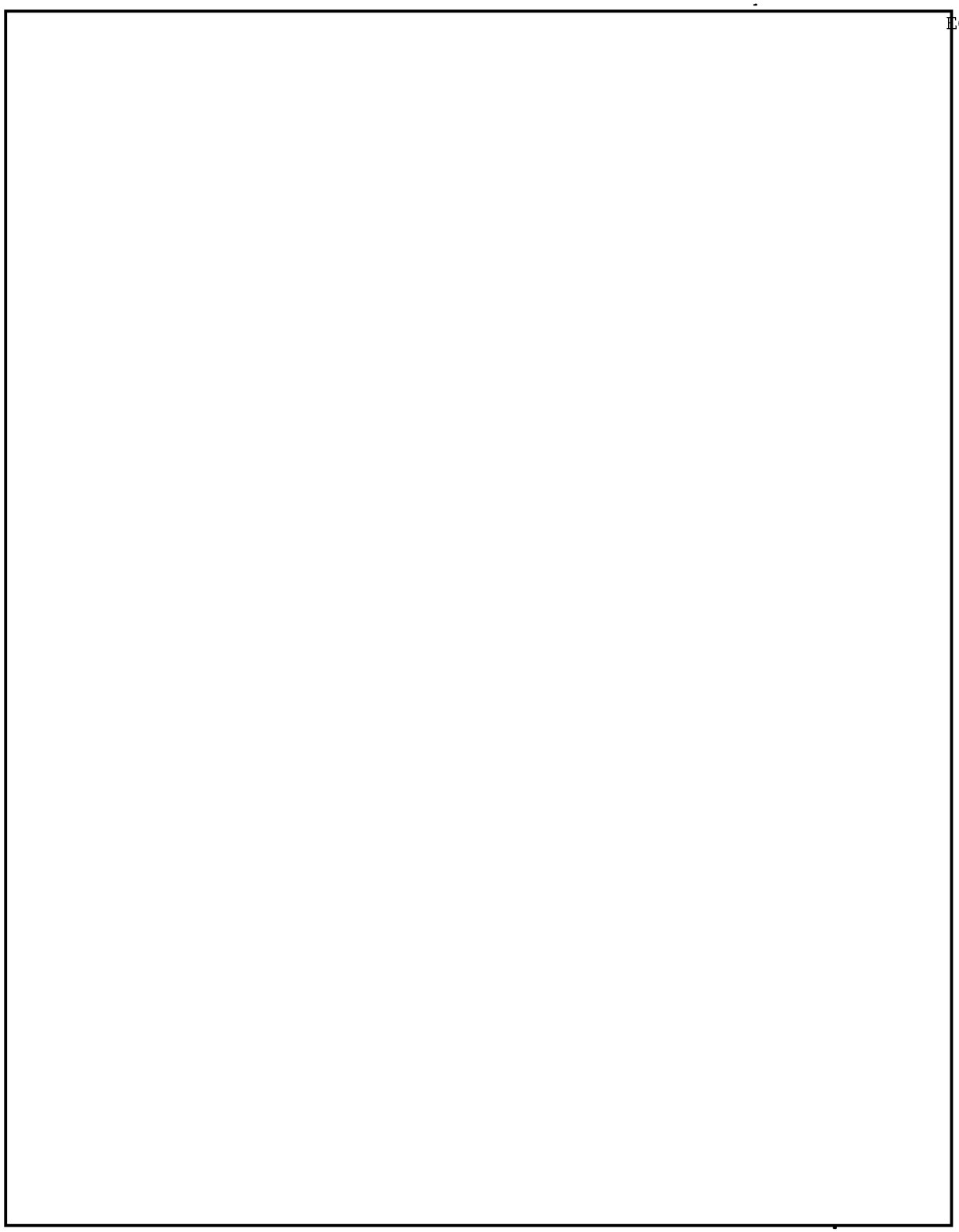
Right now, if I have a very large vocabulary in a standard two-part code, it may run up to 32 pages or more. (The largest is 64 pages). If I have to insert say a half-dozen code values for every plaintext entry, my code book gets to be about 200 pages long, rather awkward to jam in the most voluminous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

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

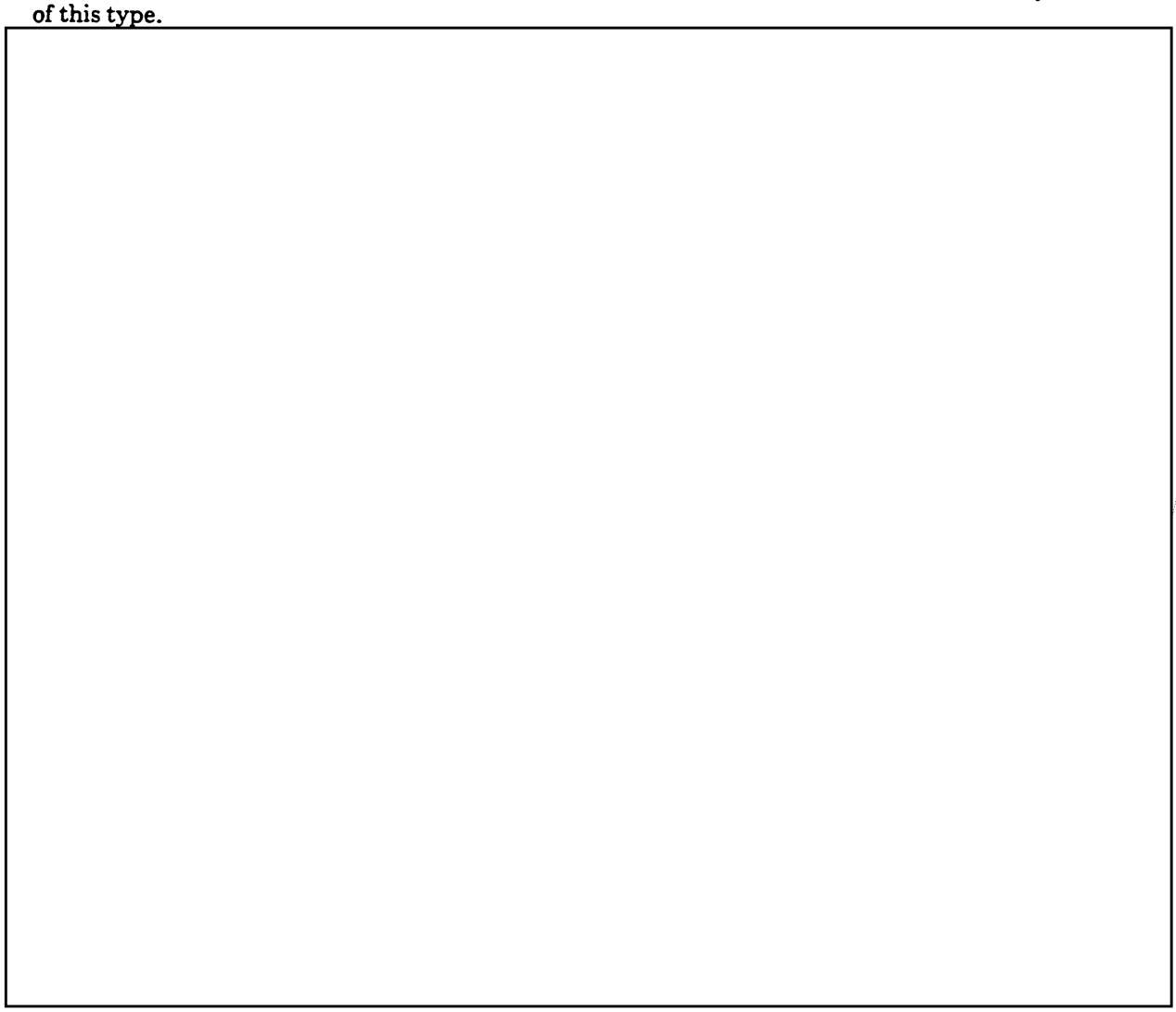
holder net—10,000 for 100 holders! So limitation number two: the size of a net that you can practicably operate in this way is very small: preferably just two stations.

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

EO 1.4 (c)



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



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

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

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

I

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

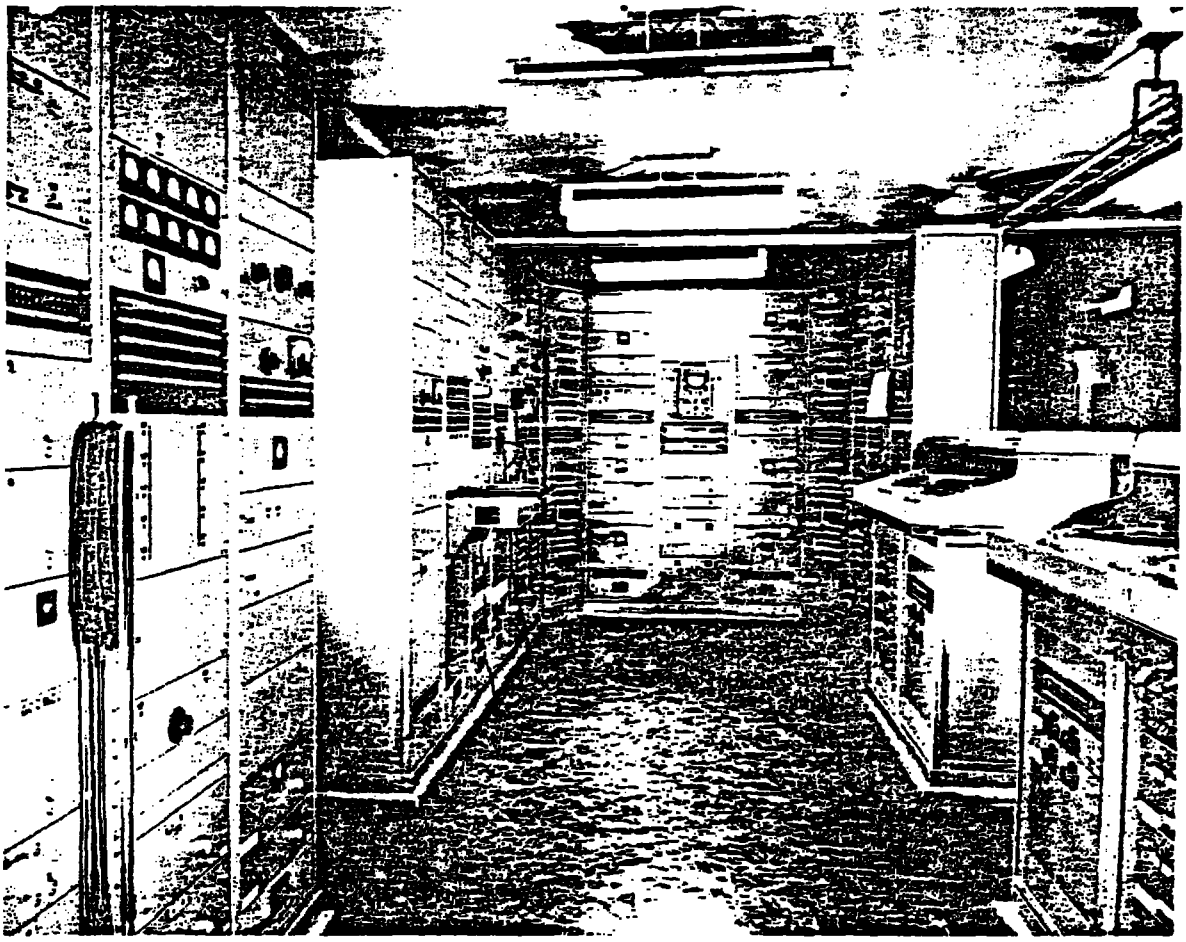
EO 1.4.(c)

EO 1.4.(c)

SEVENTH LECTURE: Ciphony Equipment and Other Specialized Systems

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

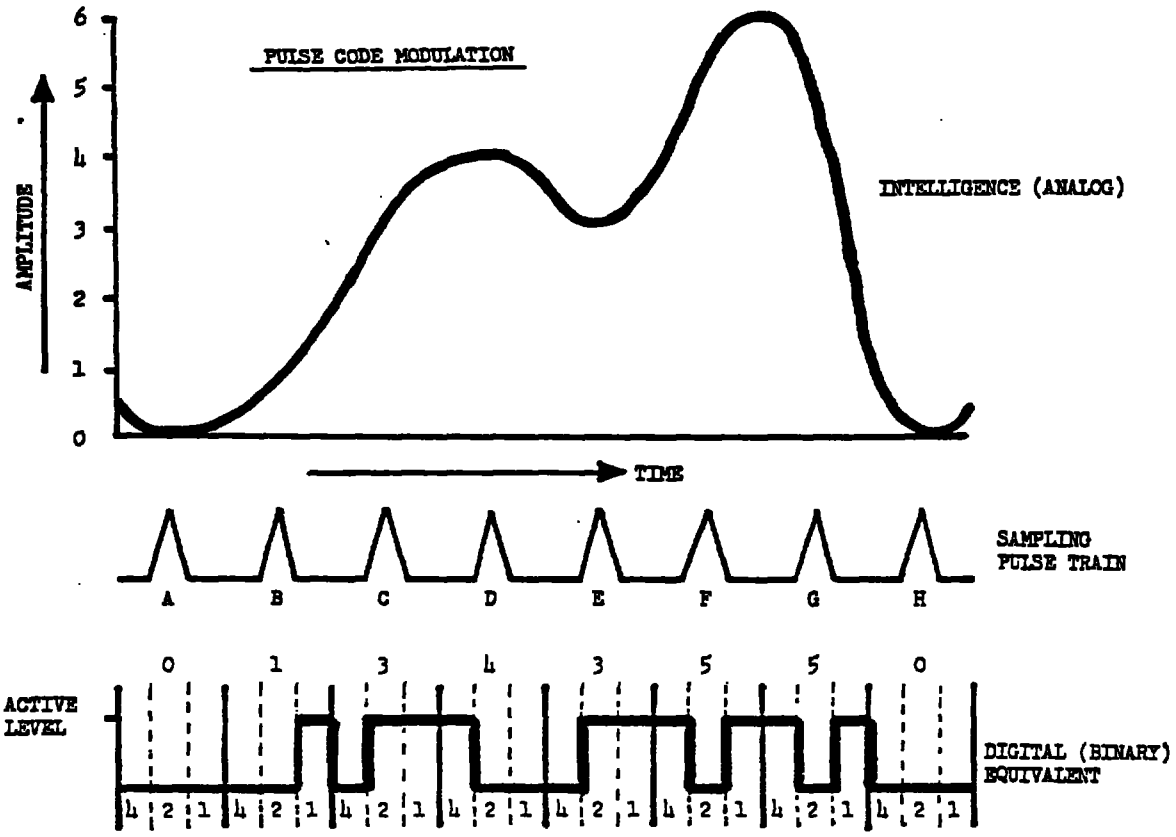
We have to go back to World War II for a look at our first voice encryption equipment:



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

The next ciphony system to come along was called the AFSAY-816. It was designed to operate over microwave links—actually, just one link—between the Naval Security Station and Arlington Hall. Since there was plenty of bandwidth to play with (50 KHz), there were no constraints on the number of digits that could be used to convert speech into digital form. The technique used was

called Pulse Code Modulation (PCM): conceptually, it involves sampling the amplitude (size) of an intelligence signal, such as one's voice, at fixed intervals of time determined by a high frequency pulse train, then transmitting the values thus obtained in some sort of binary or baudot code. The following illustration portrays these relationships:



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

EO 1.4

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

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

unintended location. As a matter of fact, there was a "permanently" anomalous situation over parts of Southeast Asia that caused VHF communications to double their expected range.

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

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

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

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

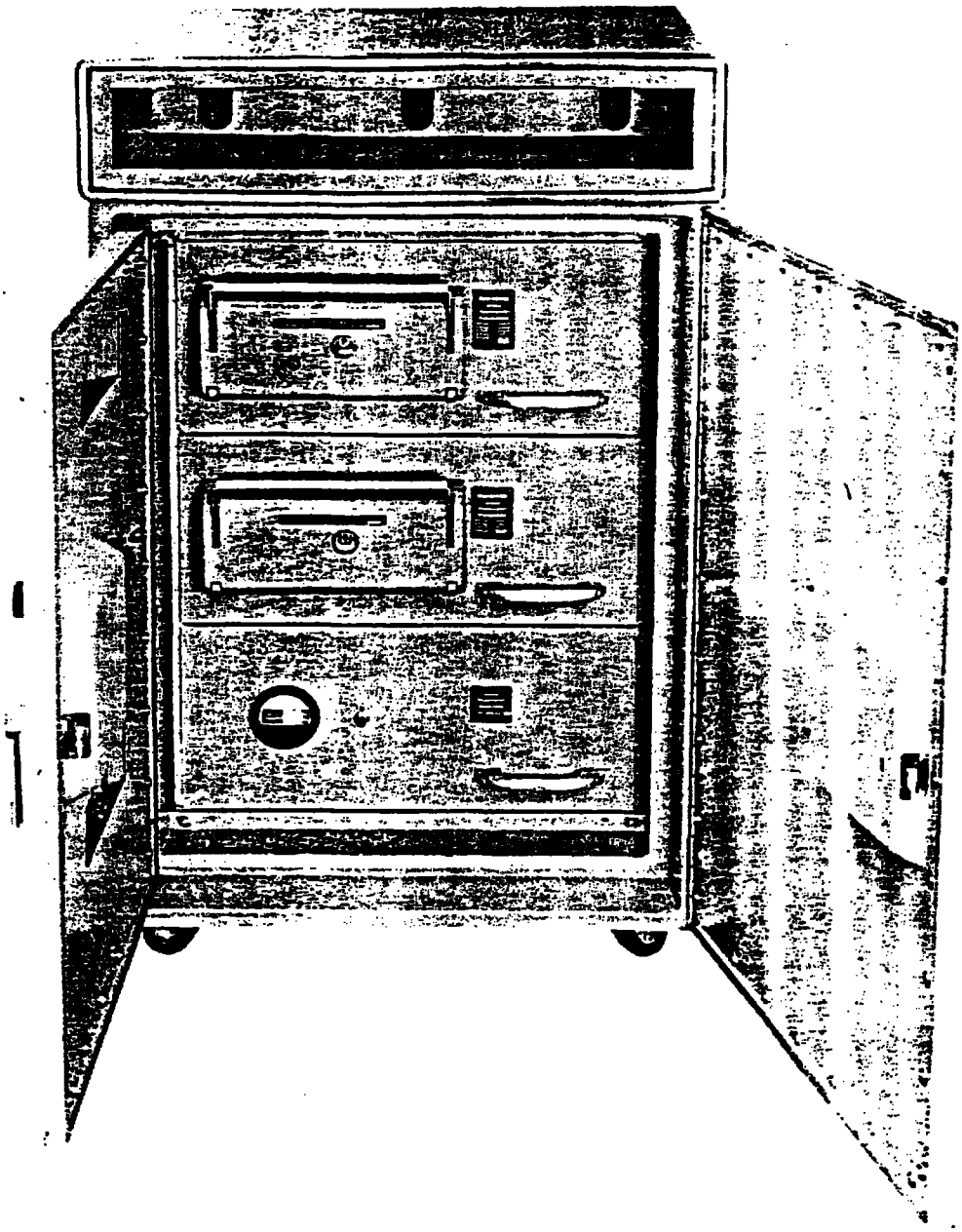
The resultant product was called the TSEC/KY-1. The most striking feature it had, in contrast to its predecessor ciphony devices, was that it was neatly packaged in a single cabinet about two-thirds as tall and somewhat fatter than an ordinary safe. Because it was built not to be in a cryptocenter or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

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

EO 1.4.(c)

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

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



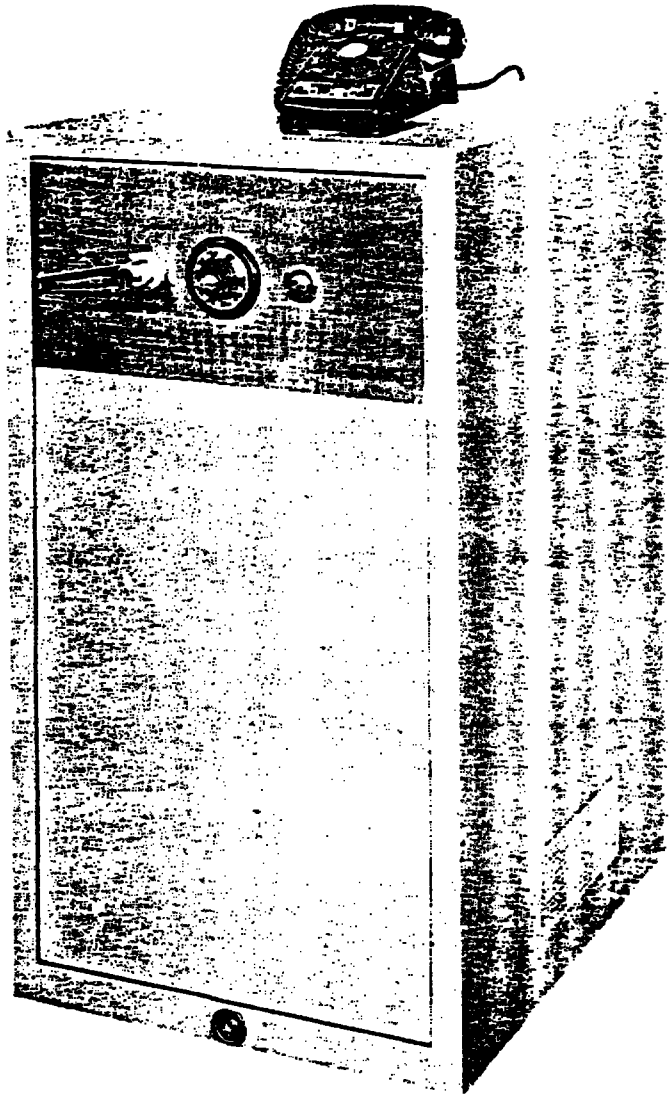
This is perhaps as good as a place as any to go off on another of the tangents that seem to characterize these lectures. As we have been following the evolution of U.S. cryptography, I have talked

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

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

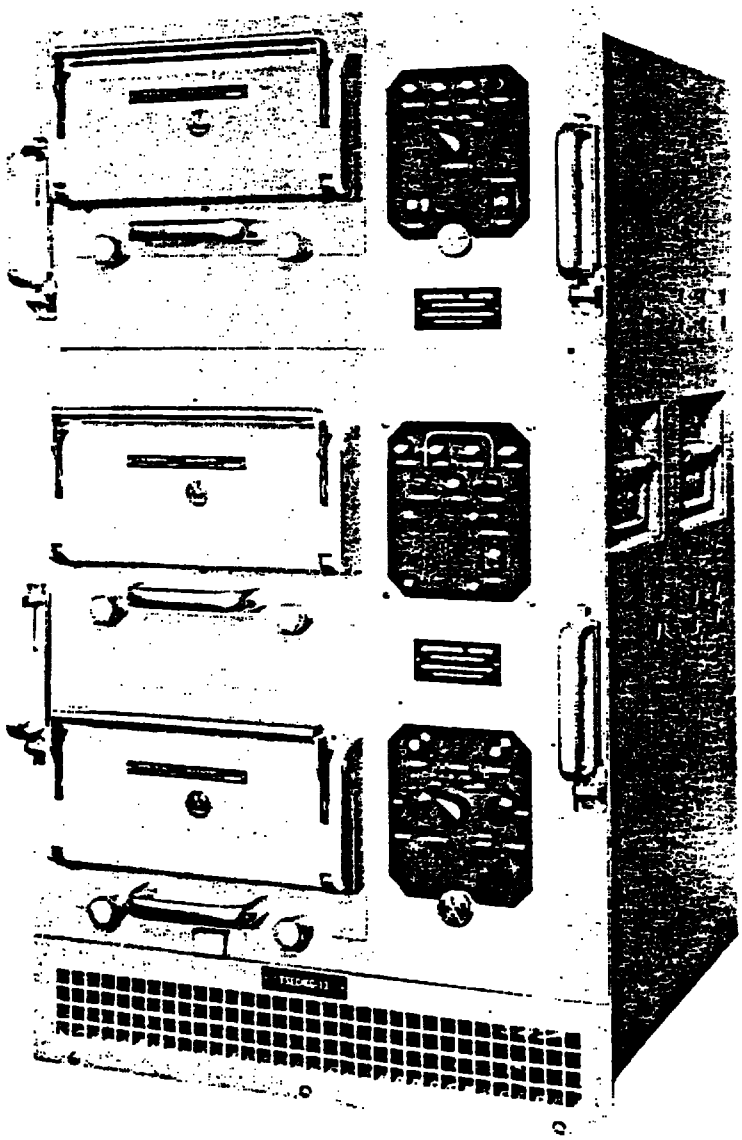
So, at the same time these wide-band fixed-plant equipments are being developed, we were working on something better than the KO-6 to satisfy long-range, narrow-band communications requirements, something that could, hopefully, be used on ordinary telephone lines or on HF radio circuits overseas. (Ma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

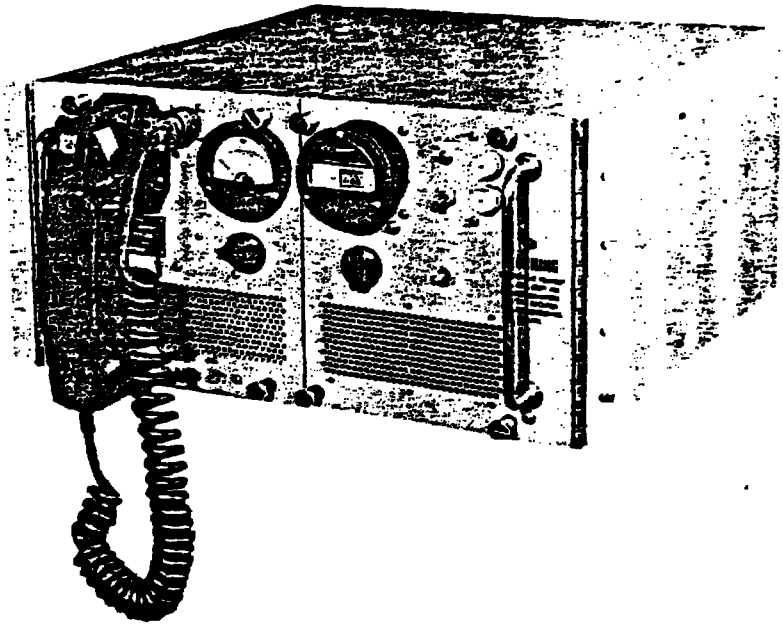
The equipment which evolved is called the KY-9.



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

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





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

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

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

and subscribers were held to SECRET unless they were essentially co-located with the crypto-equipment itself.

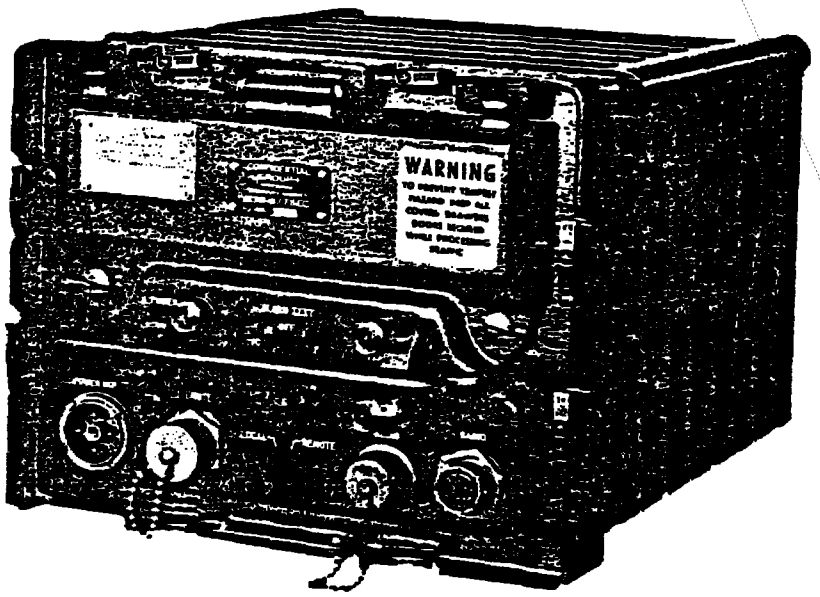
Tactical Ciphony.—MC's for tactical ciphony equipment—be they broad-band, narrow-band, or somewhere in between—have existed since before this Agency was created. But the difficulties were terrific. To have tactical usage on field telephones and radio telephones and military vehicles and, especially,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

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

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

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

EO 1.4.(c)



EO 1.4.(c)

[redacted]

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

[redacted]

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

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

[redacted]

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

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

Specialized Systems.—There are two other types of systems now in the inventory beyond those I have described that I want to touch on briefly. I have left them till last because they are among the most specialized and have as yet seen relatively little use in comparison with the big systems we have talked about. The first of these is the KG-24, designed for the encryption of TV signals—civision we call it. With the requirement for encrypting TV signals, we found ourselves faced with the problem of generating key at extremely high speeds, even by computer standards. So far, the fastest system I have described to you was the old AFSAY-816 with a bit-rate of 320 KHz—but this took six bays of equipment and had security, operational, and maintenance problems almost from the outset. Among the modern systems, the KG-3/13, with bit rates up to 100 kilobits was the fastest. But, as you know, with your home TV set, you tune to megahertz instead of kilohertz and it takes millions of bits each second to describe and transmit these TV signals. The KG-24 does it, and in one fairly large cabinet.

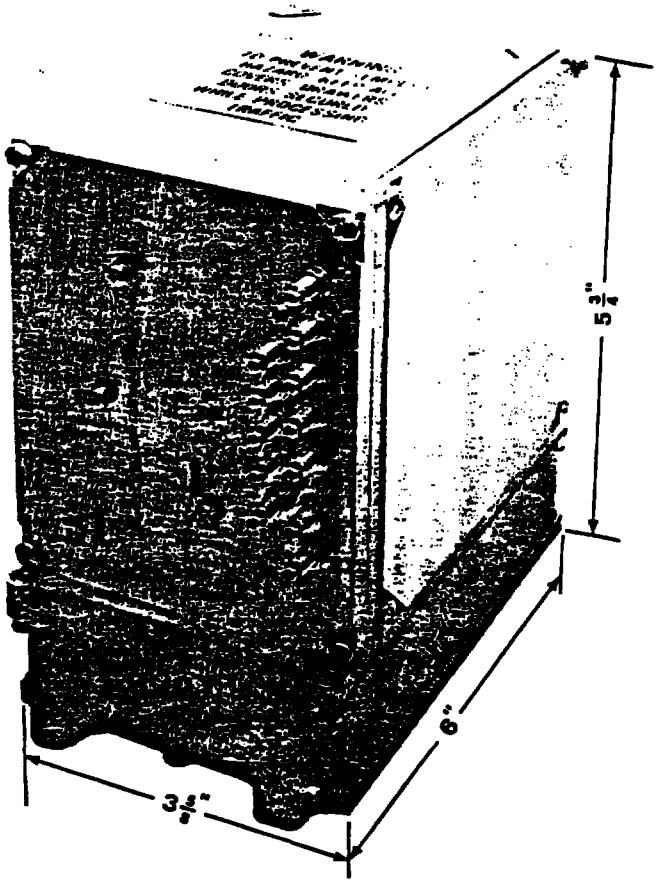
[redacted]

But there are only 6 (V-1) and 7 (V-2) models in existence, and further procurement is not planned. The main thing wrong with it is simply that it costs much too much.

The second type of modern specialized system I want to talk about is the family of equipment designed specifically to go into space vehicles. There were some obvious and some not-so-obvious difficulties that had to be met in the design of these equipments. One obvious problem was to make them small enough, and this requirement gave a big push to our general work in the micro-miniaturization of hardware. The second problem was also inherent in space technology—that was the need for extreme reliability. For unmanned surveillance satellites, if the system fails, you can't call a maintenance man. So we were faced with more rigid specifications and quality controls than we

had ever seen before. The third problem has to do with the extraordinary complexity of satellite systems as a whole. We have found it next to impossible to provide decent crypto-equipment for our customers without a very full understanding of the whole communications and operations complex in which they are to operate. With our limited manpower, this has proven difficult enough to do with modern conventional communications systems and switching complexes on the ground but, for the space requirements, we had to educate our people to speak and understand the language of this new technology; and we have a little group who live and breathe this problem to the exclusion of nearly everything else.

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



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

...eir original alignment again, and the daily change of its key was incorporated mainly to limit the scope of any loss that might occur—that business of supersession and compartmentation again.

So far, these things are working well—one technical security problem has been encountered.

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

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

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

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

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

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

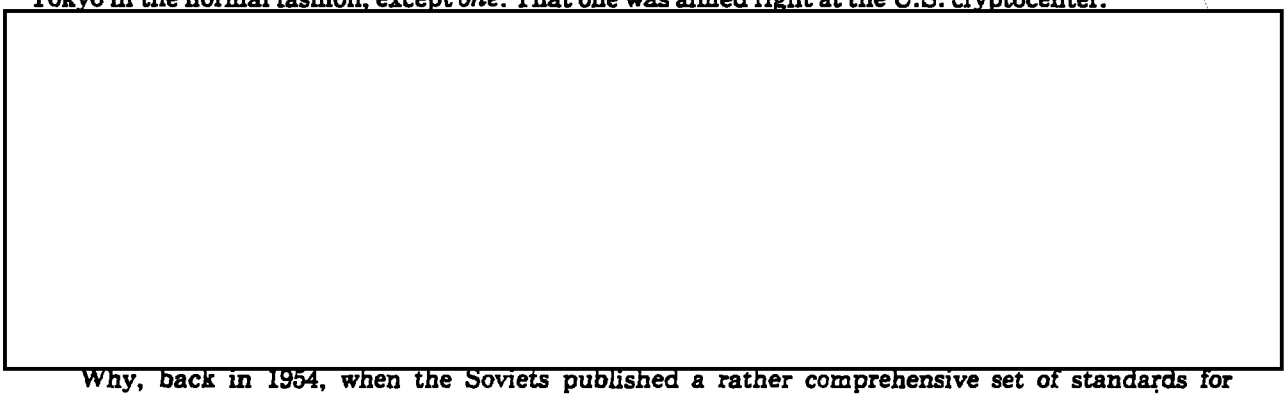
EO 1.4.(c)

EO 1.4.(c)

EO 1.4.(c)

TENTH LECTURE: TEMPEST

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



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

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

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

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

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

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

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

The three basic supression measures Bell Labs suggested were:

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

The trouble with these solutions, whether used singly or in combination, all stems from the same thing: that is the fact that, quite typically, these compromising emanations may occur over very large portion of the frequency spectrum, having been seen from near d.c. all the way up to the gigacycle range (and that's a lot of cycles). Furthermore, 5 copies of the same machine may each

exhibit different characteristics, radiating at different frequencies and with different amplitudes. And even the same machine may change from day to day as humidity changes or as contacts become pitted, or as other components age. This means that any shielding used must form an effective barrier against a large variety of signals, and this proves difficult. Similarly, the filter has to be a nearly perfect one and they become big, heavy, and expensive. Furthermore, on signal lines for example, how do you get your legitimate cipher signal through without compromising signals squeezing through with them?

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

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

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

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

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

At the same time we were scurrying around trying to cope with the 131–B2 mixer, we thought it would be prudent to examine every other cipher machine we had to see whether the same problem existed. For, way back in the late 40's, Mr. Ryon Page and one of his people were walking past the cryptocenter at Arlington Hall and had heard the rotor machines inside clunking away. He wondered what the effect would be on the security of those systems if someone were able to determine which rotors or how many rotors were stepping during a typical encryption process. In due course, some

assessments were made on what the effect would be. The assessments concluded that it would be bad, and they were filed away for future reference. Now, it appeared that there might be a way for an interceptor to recover this kind of data. So, painstakingly, we began looking at our cryptographic inventory. Everything tested radiated and radiated rather prolifically. In examining the rotor machines, it was noted the voltage on their power lines tended to fluctuate as a function of the numbers of rotors moving, and so a fourth phenomenon, called power line modulation, was discovered through which it was possible to correlate tiny surges and drops in power with rotor motion and certain other machine functions.

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

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

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

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

machine sounds with enough fidelity to permit exploitation. And such microphones were discovered in [redacted]

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

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

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

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

detected at all beyond 20 feet. The next equipment built, the KW-26, and every subsequent crypto-equipment produced by this Agency contained these circuits, and a great stride had been made.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

physical and electrical separation between those circuits carrying classified information in the clear, and those carrying only unclassified information (like cipher signals, control signals, power, and ordinary telephone lines). In addition to shielding and filtering, this called for the use of conduits and often, in existing installations, drastic rearrangement of all the equipment and wiring was involved.

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

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

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

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

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

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

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

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

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

SUMMARY

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

1. We should be neither panicked nor complacent about the problem.

2. Such evidence as we have been able to assemble suggests that a few of our installations, but very few of them, are probably under attack right now. Our own experience in recovering actual intelligence from U.S. installations under field conditions suggests that hostile success, if any, is fragmentary, achieved at great cost and—in most environments—with considerable risk.

3. There remain a number of more economical ways for hostile SIGINT to recover intelligence from U.S. communications entities. These include physical recovery of key, subversion, and interception and analysis of large volumes of information transmitted in the clear. But during the next five years or so, as our COMSEC program makes greater and greater inroads on these other weaknesses, and especially as we reduce the amount of useful plain language available to hostile SIGINT, it is logical to assume that that hostile effort will be driven to other means for acquiring

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