~~COMINT~~

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

~~SECRET~~

ORIGINAL 1
Reverse (Page 2) Blank

~~COMINT~~

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.

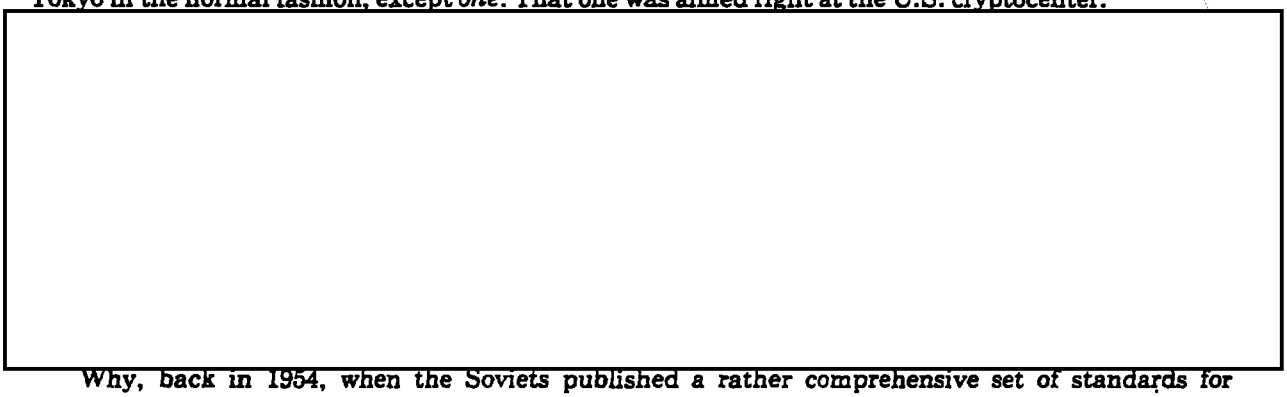
TABLE OF CONTENTS

Subject	*Page*
FIRST LECTURE.—The Need for Communications Security	9
SECOND LECTURE.—Codes	21
THIRD LECTURE.—TSEC/KL–7	33
FOURTH LECTURE.—One-Time Tape Systems	39
FIFTH LECTURE.—KW–26; KW–37; CRIB; KW–7	45
SIXTH LECTURE.—Multi-Purpose Equipment	53
SEVENTH LECTURE.—Ciphony Equipment and Other Specialized Systems	57
EIGHTH LECTURE.—Flops	73
NINTH LECTURE.—Strengths and Weaknesses	81
TENTH LECTURE.—TEMPEST	89

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.

~~SECRET~~

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

THE DAVID G. BOAK LECTURES

VOLUME II

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755

JULY 1981

~~SECRET~~

ORIGINAL
(Reverse Blank)

[redacted]

TABLE OF CONTENTS

SUBJECT	PAGE NO
INTRODUCTION	iii
POSTSCRIPT ON SURPRISE	1
OPSEC	3
ORGANIZATIONAL DYNAMICS	7
THREAT IN ASCENDANCY	9
LPI	11
SARK—SOME CAUTIONARY HISTORY	13
THE CRYPTO-IGNITION KEY	15
PCSM	17
NET SIZE	19
EQUIPMENT CLASSIFICATION	21
PUBLIC CRYPTOGRAPHY—SOME CAUSES & CONSEQUENCES	27
PKC	33
COMPUTER CRYPTOGRAPHY	35
POSTSCRIPT	37
TEMPEST UPDATE	39
SFA REVISITED	41
NESTOR IN VIETNAM	43
EMERGENCY DESTRUCTION OF CRYPTO-EQUIPMENT	47
POSTSCRIPT ON DESTRUCTION—DAMAGE ASSESSMENTS	51
TRANSPOSITION SYSTEMS REVISITED	53
MORE MURPHY'S LAW	55
CLASSIFIED TRASH	57

TEMPEST UPDATE

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

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

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

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

P.L. 86-36