~~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

~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

ORIGINAL
(Reverse Blank)

[redacted]

TABLE OF CONTENTS

INTRODUCTION

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

POSTSCRIPT ON SURPRISE

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

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

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

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

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

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

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

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

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

OPSEC

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

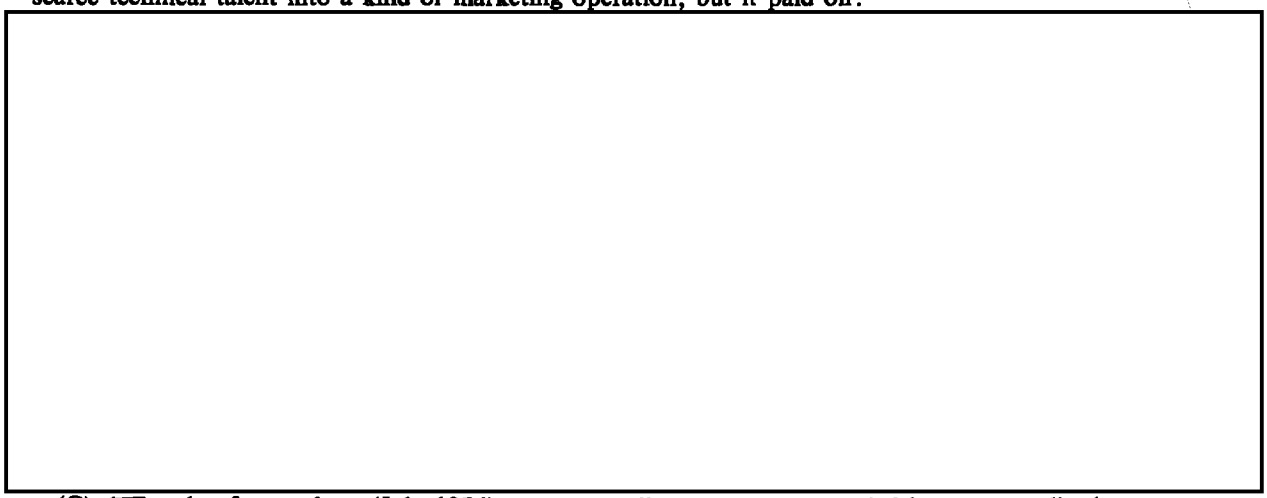
ORGANIZATIONAL DYNAMICS

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

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

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

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



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

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

~~(C NF)~~ A hoax, of course. The Navy "staffs" for them. No matter what you call it or where you put it, much of that "drudgery" has to be done. The Chief, S5 took some jibes in the form of the assertion that the only reason for the new Office was to improve, on paper, our line-staff ratio. The truth was that, quite apart from the auditor's observations,

The seven individuals in S5 and S2 most responsible got Presidential citations under a program recognizing major savings in Government. 28% of the total Government savings getting special recognition that year was the work of our people.

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

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

EO 1.4.(c)

THREAT IN ASCENDANCY

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

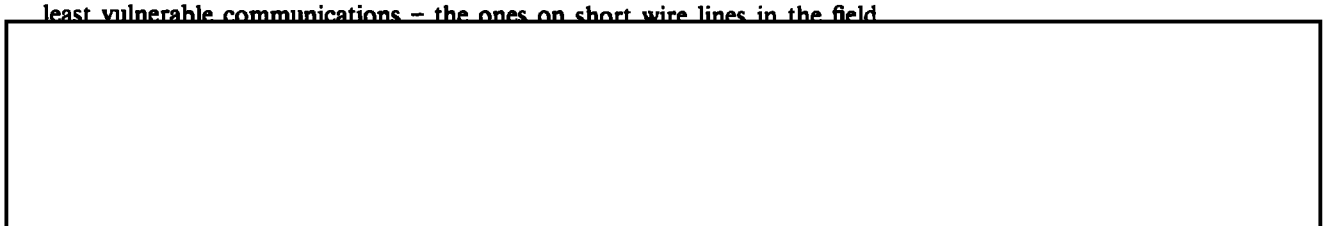
~~(C)~~ So our priorities were developed more or less in the abstract, in the sense that they related more to what we were able to do technologically or procedurally than to the probabilities that a given weakness would be exploited in a given operating environment. In short, we did not do much differentiation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

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

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

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

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



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

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

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

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

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

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

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

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

LPI

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

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

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

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

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

~~(C)~~ One of the more insidious arguments we faced in some circles where anti-jam was asserted to be more important than COMSEC arose from the fact that ordinary cryptography does not add to the resistance of a transmission to jamming. If you can jam the clear signal, you can jam it in the cipher mode. Further, a smart jammer can work against most encrypted signals more efficiently than against plain text, use less power and be on the air for much briefer intervals. This is true, because all the jammer need do is knock the cryptographic transmitters and receivers out of sync or disrupt the initialization sequences that prefix

most encrypted traffic. This is not the case where we employ CTAK (cipher text auto-key) or where synchronization is dependent on internal clocks rather than timing elements of the cipher text itself. All the others are vulnerable if the jammer can stop them from getting into sync in the first place by repeatedly attacking preambles.

SARK—SOME CAUTIONARY HISTORY

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

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

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

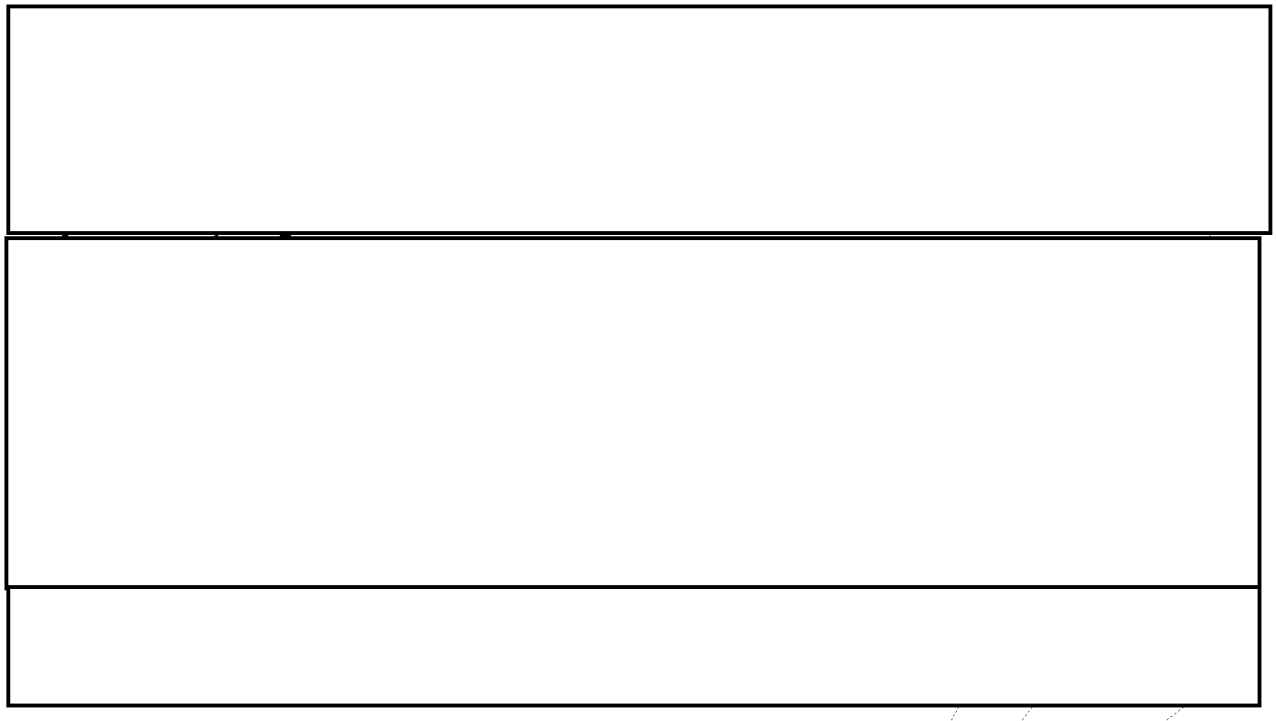
~~(C)~~ For a typical, small, tactical radio net (10–20 holders) the idea was that each subscriber would either go to net control and have his equipment loaded with his variables, or net control would dispatch a courier with an ETD to load his variables *in situ*. Thereafter, he would operate independently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

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

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

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

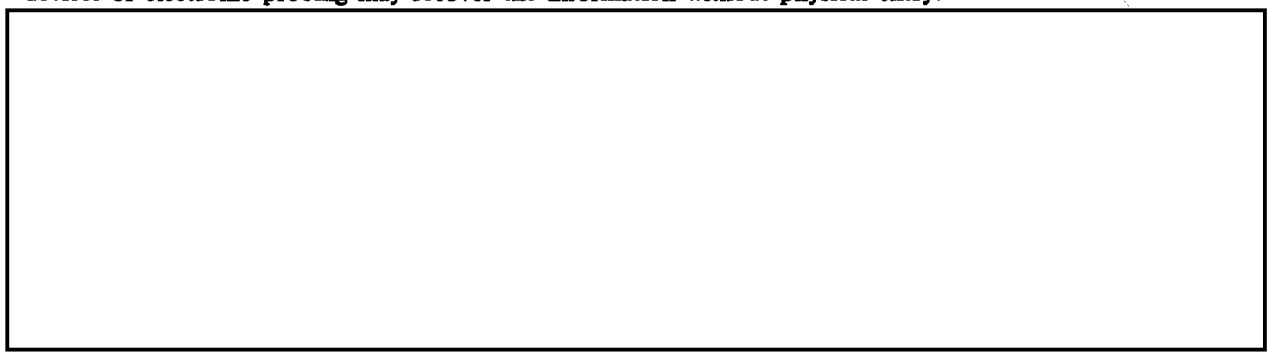
THE CRYPTO-IGNITION KEY



P.L. 86-36

PCSM

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



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

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

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

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

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

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

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

NET SIZE

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

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

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

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

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

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

EQUIPMENT CLASSIFICATION

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

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

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

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

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

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

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

[redacted]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(C) In any event, most people in S are pretty well sensitized and/or resigned to the need for protecting logics and precise information about their strengths and weaknesses. However, that is not the case with

large batches of peripheral information about how we obtain communications system security. We tend to play fast and loose with information about alarm structures, about "TRANSEC" features, depth protection, anti-jam protection, cryptoperiods, keying techniques, testing, financial and logistics arrangements, parts catalogs, plans, schedules, operating instructions, physical safeguards, and usage doctrine in general.

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

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

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

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

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

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

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

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

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

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

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

~~(C CCO)~~ So, one root question we need to ask ourselves when we are trying to decide whether something need be classified or not is: "What would be the value of the information if I were part of a hostile SIGINT organization – any such organization?" "Will its protection block or delay potential efforts against us?" A correlative question – equally difficult for COMSEC people to answer – is: "will it be useful to an actual or potential US SIGINT target by showing that target something it can use to improve its own COMSEC

equipment or procedures?" "What would our own SIGINT people give for comparable information about targetted foreign cryptography?" A trap to avoid in attempting that answer is conjuring up only the Soviet Union as the "target" in question. Clearly, there are categories of information which would be of little use to them because of the level of sophistication they have already achieved in their own cryptography, but could be of extreme value to other countries.

[redacted]

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

EO 1.4.(c)

PUBLIC CRYPTOGRAPHY—SOME CAUSES & CONSEQUENCES

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

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

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

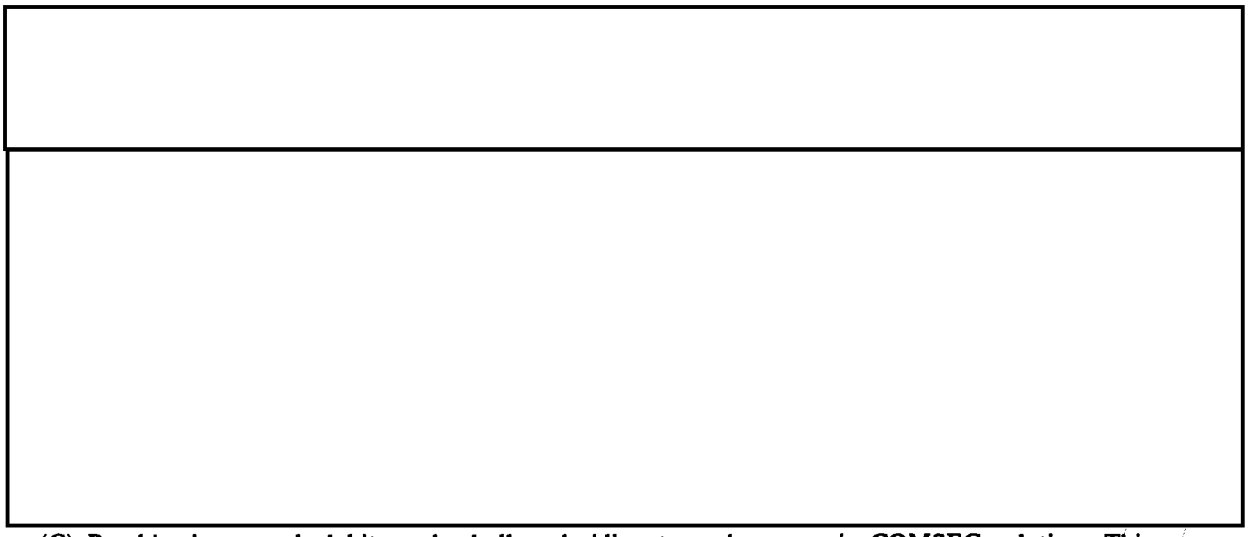
~~(S)~~ A handful of U.S. companies interested in computers, in communications, or in electronics began to perceive a market for electronic crypto-equipments. A few other American companies began building crypto-equipment in competition with the Swiss and others in Europe, supplying devices to some Governments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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

~~(C)~~ Through all this controversy, and notwithstanding our security concerns (some will read "paranoia"), there is a very strong motivation among us for cooperation with DoC, with Industry, and with the Academic

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

EO 1.4.(c)

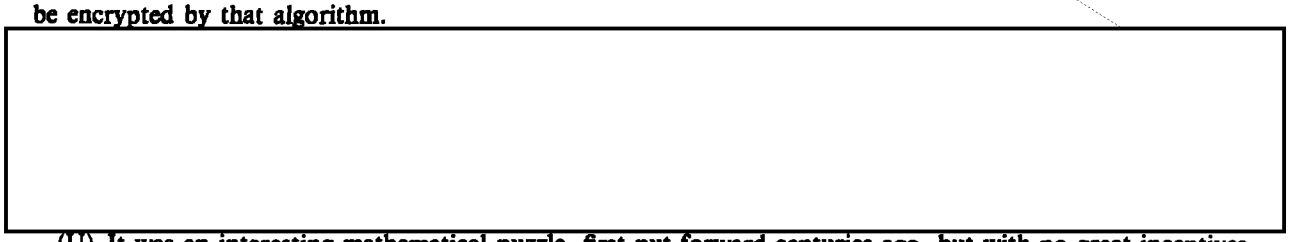
EO 1.4.(d)

PKC

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

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

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



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

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

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

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

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

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

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

COMPUTER CRYPTOGRAPHY

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

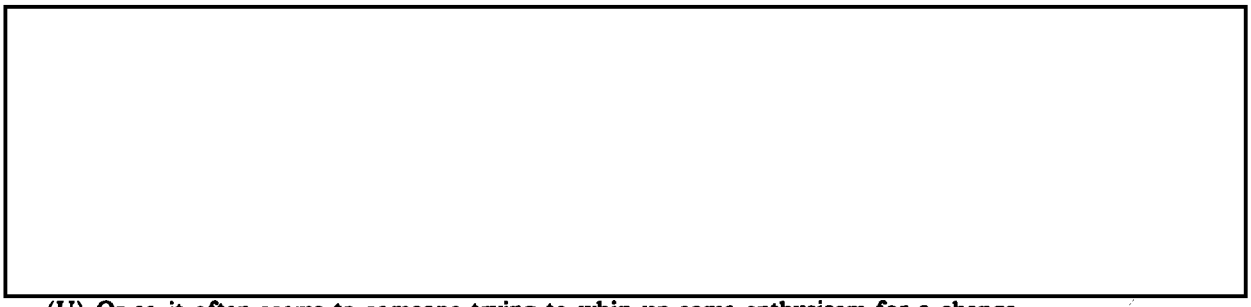
~~(C)~~ Nevertheless, there has been little proliferation of computer cryptography in the ensuing years, mainly because the inherent constraints in the BRN-3 environment (excess capacity, system high operation, receive mode only, and rigorous access control) are still not prevalent. The security problems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

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

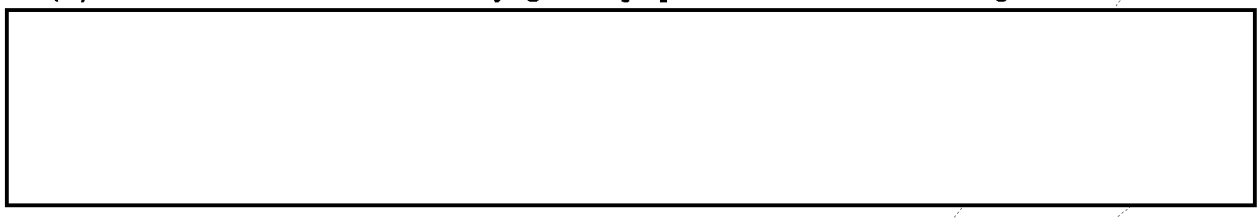
~~(C)~~ Two other factors have slowed the rush towards computer cryptography. The first is that most commercially available computers still have TEMPEST problems. Few meet our TEMPEST standards for crypto-equipments (KAG-30), and they are difficult to fix. The other factor is that the dedicated (special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

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

POSTSCRIPT



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



EO 1.4.(c)

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.

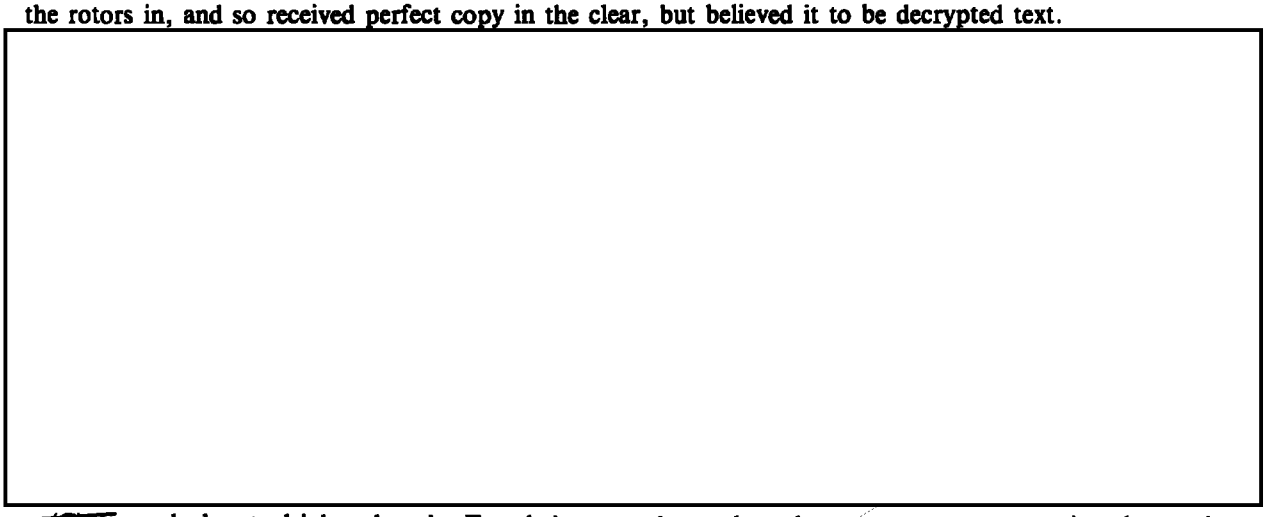
P.L. 86-36

SFA REVISITED

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

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

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



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

P.L. 86-36

NESTOR IN VIETNAM

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

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

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

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

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

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

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

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

~~(C)~~ There was a shortage of cables to connect NESTOR to its associated radio. This sounds like a small and easily solvable difficulty; but it turned out to be one of the biggest and most persistent we had. It stemmed from a deeper logistics problem because different organizations were responsible for fielding the various components that went into a secure tactical system. We procured the NESTOR equipment. Various Service organizations procured the various radios with which it was used; and still different organizations fabricated cables and connectors to link them up. Systems planners and implementers in Vietnam eventually

gave up and appealed to CINCPAC to orchestrate a coherent program. CINCPAC gave up and appealed to JCS (who may have done a staff study), and it was never solved.

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

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

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

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

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

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

1—Speeds up and improves operations
2—Slows down and interferes with operations
3—Has little or no affect on unit effectiveness

OGA

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

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

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

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

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

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

E—Other (Specify)

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

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

1—Yes, to a considerable degree

2—To some moderate degree but not significantly

3—No

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

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

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

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

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

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

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

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

G—TSV equipment is not reliable in critical situations.

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

I—Other (Specify)

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

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

EMERGENCY DESTRUCTION OF CRYPTO-EQUIPMENT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

POSTSCRIPT ON DESTRUCTION—DAMAGE ASSESSMENTS

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

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

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

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

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

TRANSPOSITION SYSTEMS REVISITED

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

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

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

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

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

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

(S) Part of the difficulty may have been that the only formal, objective crypto-security *standard* ever published in S is the High Grade Standard for equipments – systems meeting that standard are essentially approved for any type of traffic you might specify for their fifteen or twenty year life. No intermediate or "low-grade" standard has been adopted, despite yeoman efforts to devise one. Ironically, even among the high grade systems, there is considerable variation in their overall security potential – some provide transmission security; some do not. Some are heavily alarmed; some have little protection against failure. Some have full TEMPEST protection; TEMPEST standards were waived or moderated for others. The difference with PARKHILL may be that it is the first equipment from which at least fragments of plain language may be recoverable at lower cost and in less time than possible with any other equipment, even when it is working perfectly. But, again, remember, the alternative.

(S) A further irony is that while a real dilemma is seen with PARKHILL, we have accepted – mostly blandly – a large inventory of manual systems, many of which can be broken with relative ease. In their case, we have accepted, perhaps too uncritically, the idea that the systems themselves place limits on the

kind of traffic they can process. At this writing, however, rumor has it that there is a sub-rosa paper authored by a fresh face entitled something like: "Manual systems – Are they Worth the Paper They're Printed On?" COMSEC will be well-served with critical re-examination of old ideas and quite a batch of hoary premises (including some in Volume I!), particularly by our new people. Just be sure of your facts.

MORE MURPHY'S LAW

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CLASSIFIED TRASH

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

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

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

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

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

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