~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

APRIL 1979

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 1 April 2009~~

~~SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. VI, No. 4 APRIL 1979

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~SECRET~~

COMSEC/SIGINT Relations (U)

David G. Boak, S

Last November, David Boak, Special Assistant to the Deputy Director for Communications Security, NSA, presented an address on the status of COMSEC today to the members of the Communications Analysis Association. CRYPTOLOG *is pleased to be able to pass Mr. Boak's observations on to a wider audience.*

"...the good old KL-7, the only cipher machine we have left that looks like a cipher machine--the only one that's sexy at all."

(U) The easiest way to describe COMSEC is to say that it counters SIGINT. Our job in S is to frustrate the SIGINT professionals in hostile governments. Another way of looking at COMSEC, perhaps a more positive one, is to answer the question, "What's it for?" In a nutshell, I think that what COMSEC is for is to help the government achieve surprise. Now, I don't just mean the classical military tactical and strategic surprise, although, of course, that's crucial—but technological and diplomatic surprise as well.

~~(C)~~ I believe that the SIGINT element of the national intelligence community remains the pre-eminent one. And the reason I do is that SIGINT provides to our decision makers the most timely, most authoritative, most accurate (and often unique) information those decision makers get about what the other guy is going to do before he does it.

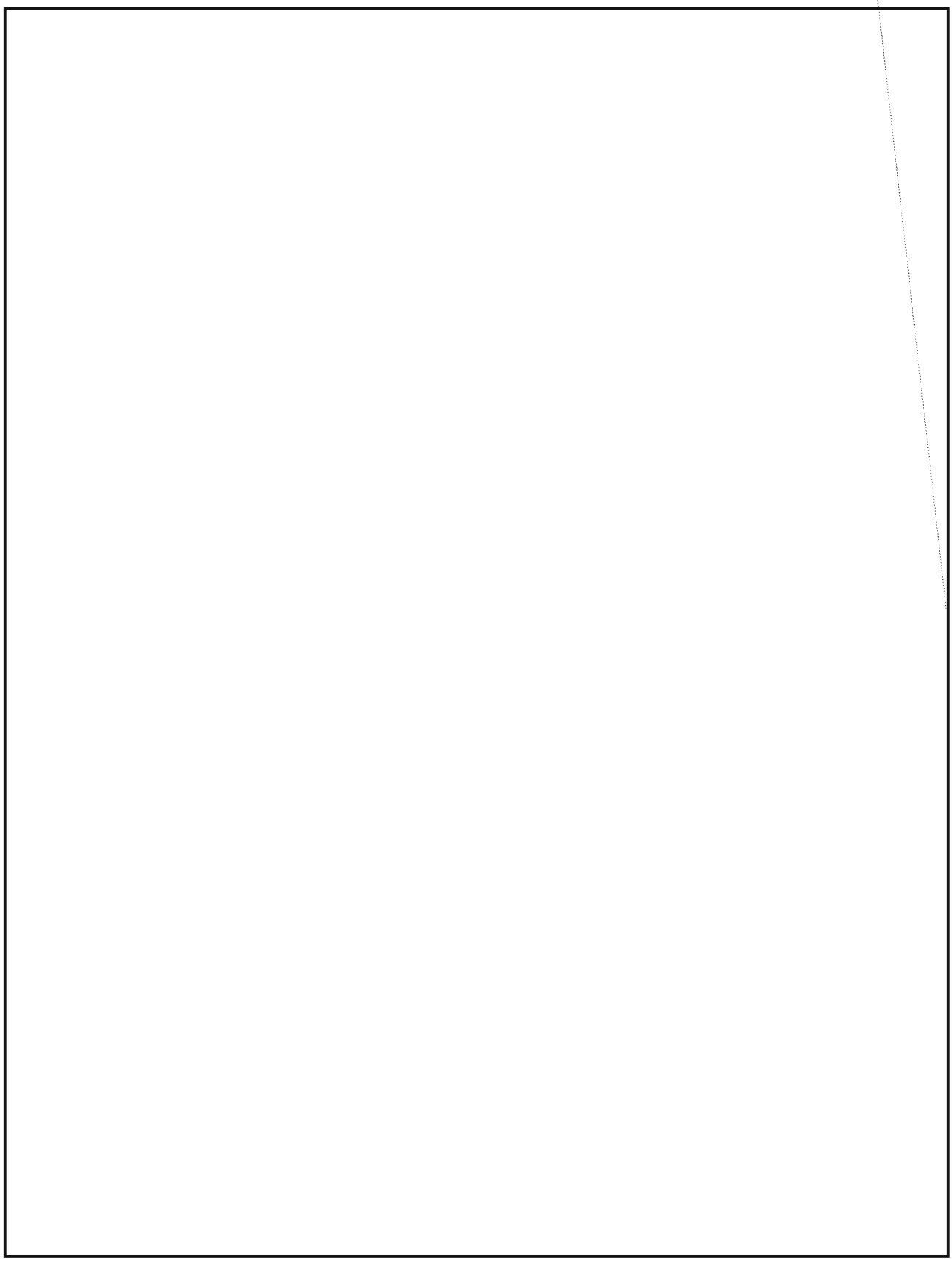
There are a few examples where we can demonstrate that a modest handful of COMSEC devices saved tens of millions of dollars in support of big operations, and some dismal instances in which we can show that the lack of COMSEC cost many lives. I suggest, therefore, that it is an excellent investment.

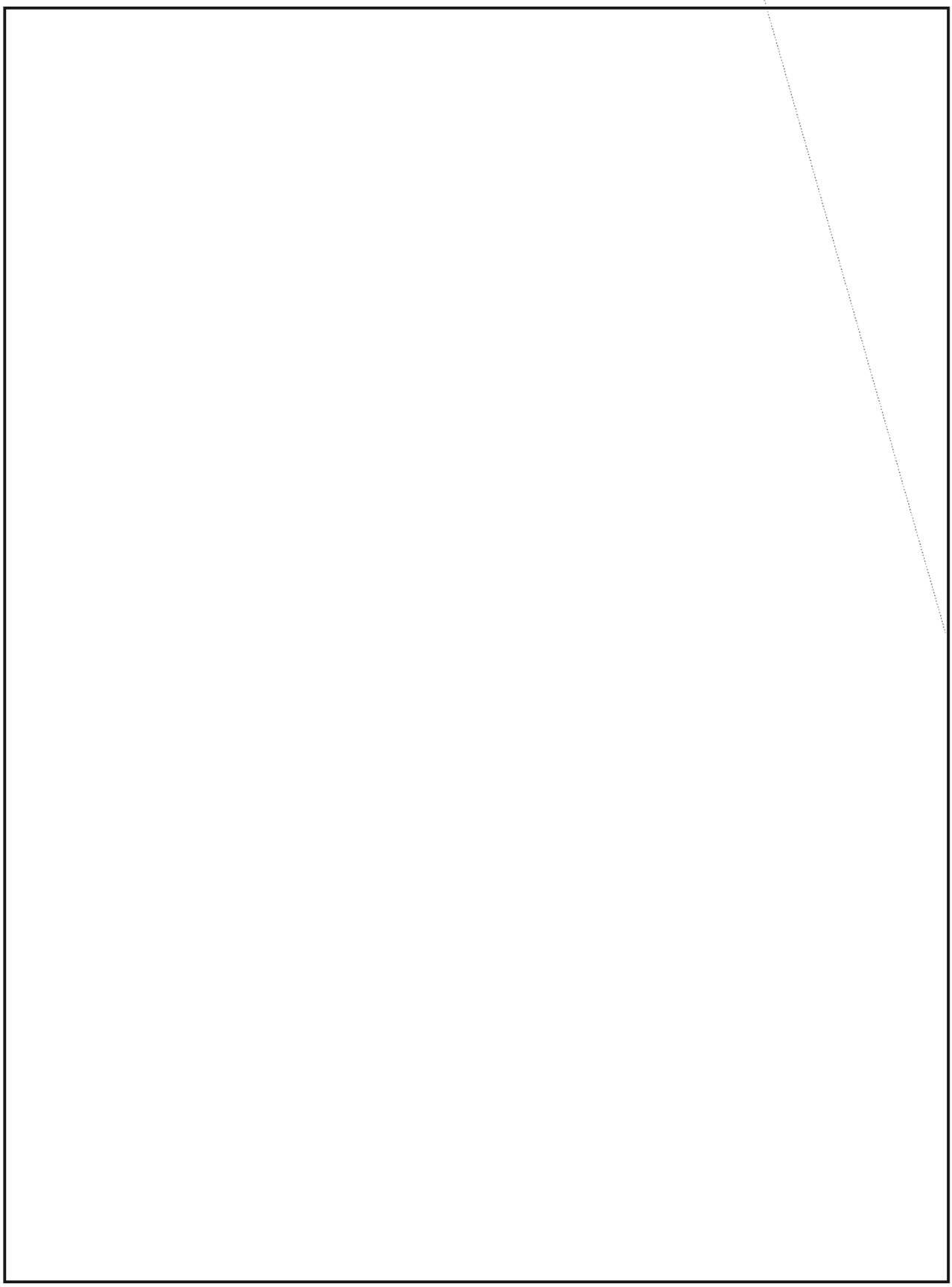
(U) Now, let's see what we're up against in trying to do that job.

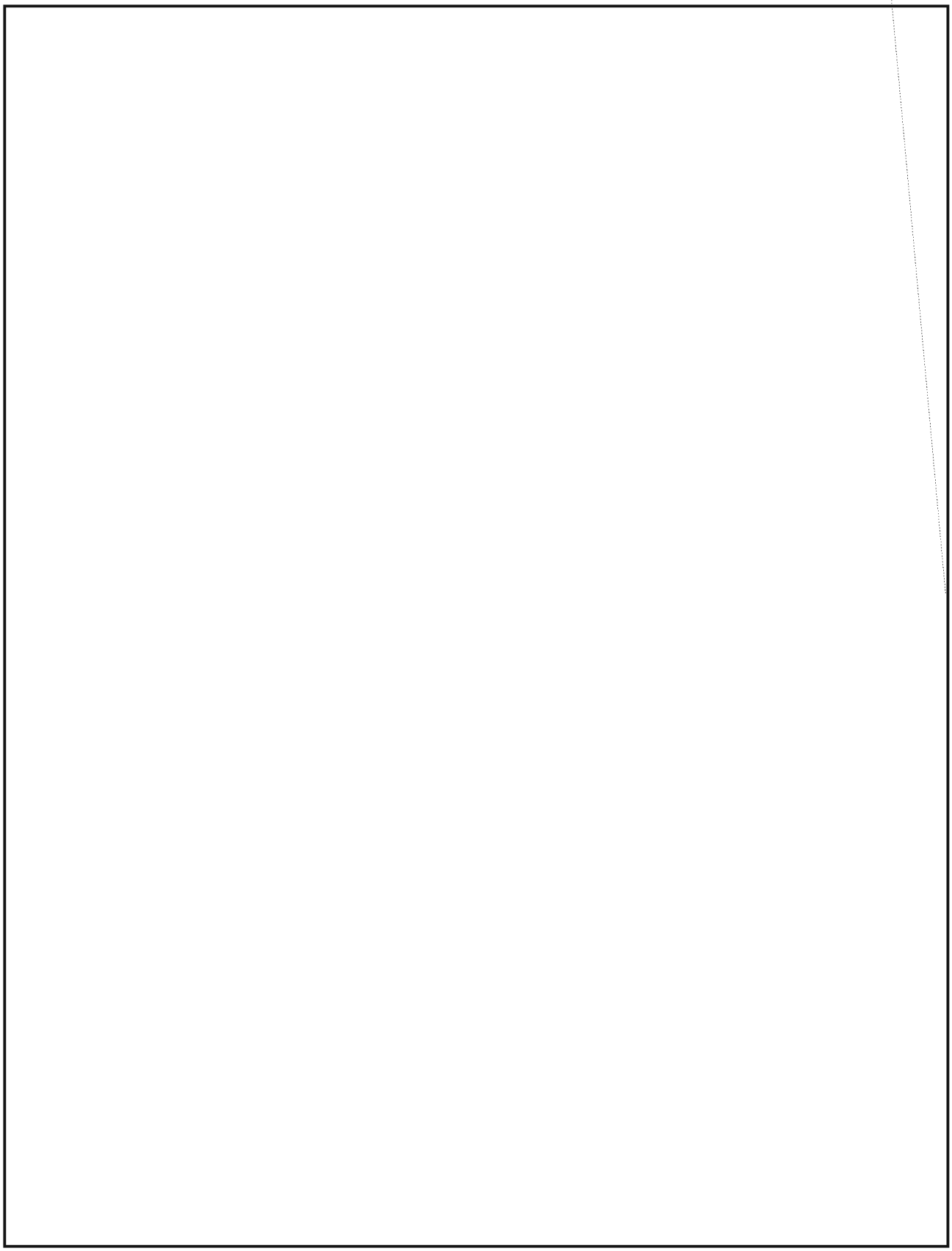
~~(C)~~ *The Threat*. Until the early 1970s this Agency had no coherent, comprehensive picture of what COMSEC was up against. We had fragmentary information. We got some of it from the SIGINT world and some from other sources. But, by and large, it was catch-as-catch-can. We assumed the worst about that threat and did the best we could to cope with it in an unstructured way.

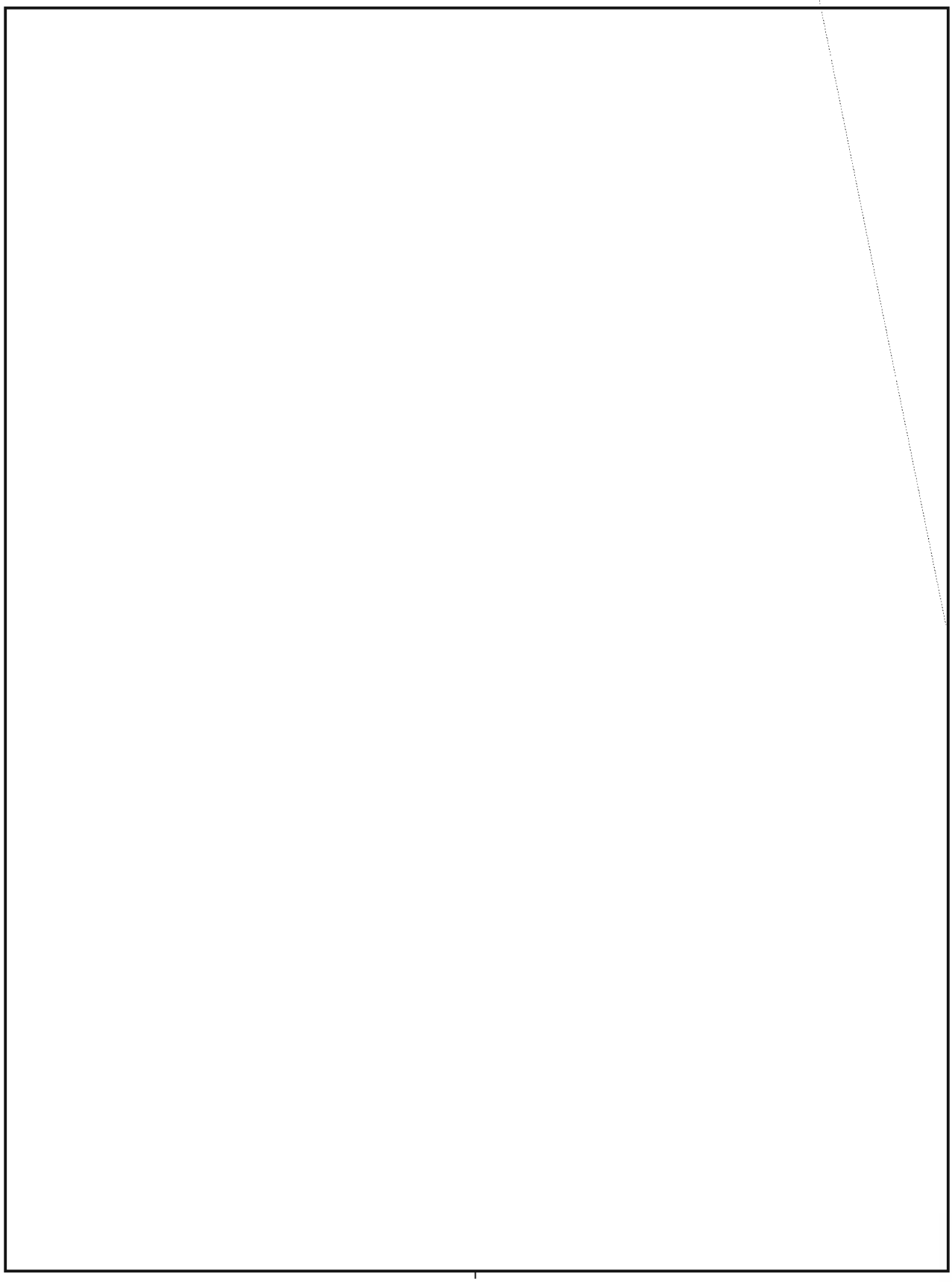
~~(C)~~ But we began to realize that our COMSEC assets were finite and that we had to allocate the resources, people, and machinery, as well as new developments, to optimize our position against the threat. And the better we could define it, the better we could get the right systems to the places where we were hurting the most. Therefore, we built an entire division with a specific mission of determining what we're up against, helping us assess what that meant to us, helping with our plans and our prioritizations. We could then begin to allocate such assets as we had on an educated basis.

~~SECRET~~

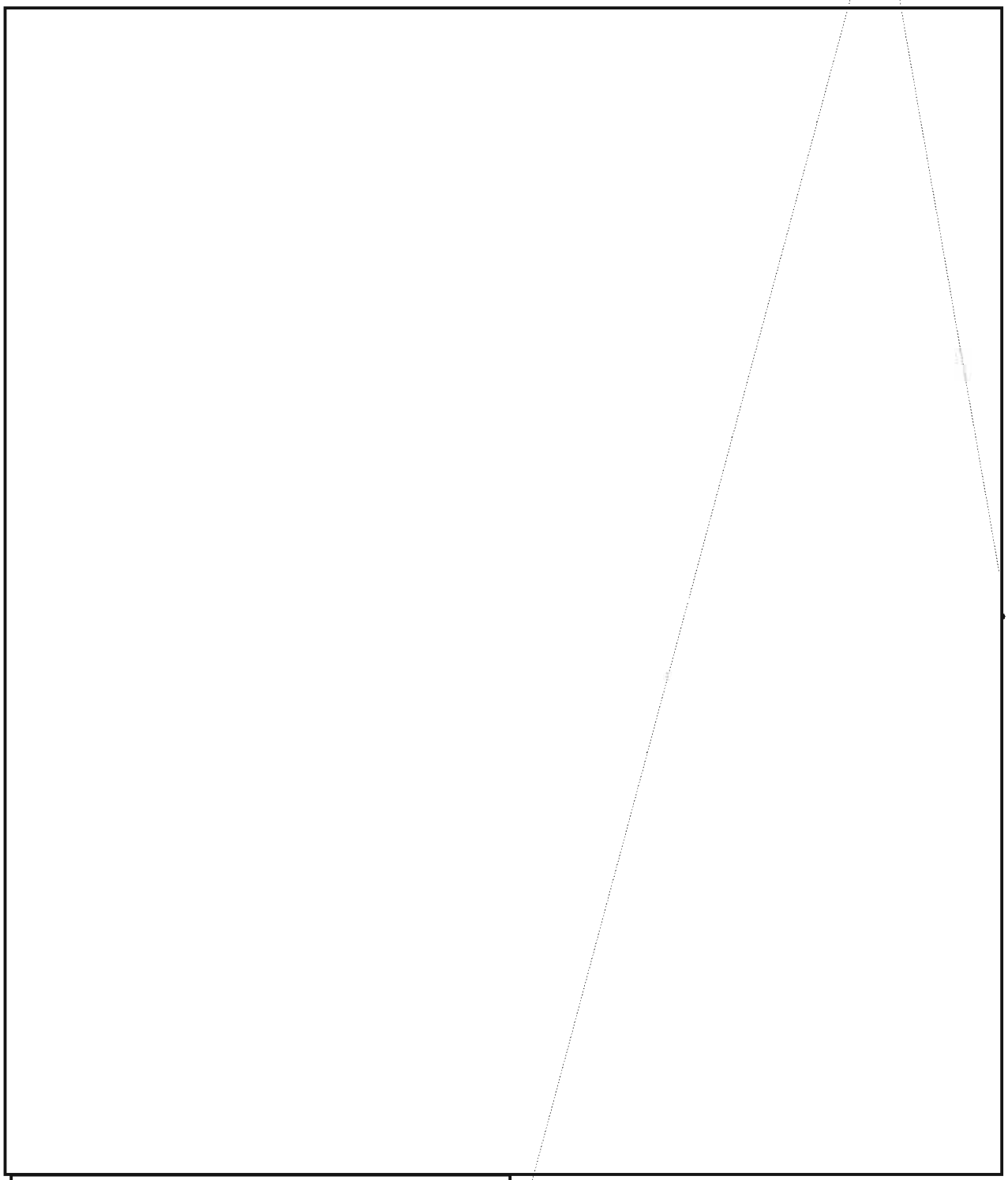








~~SECRET~~



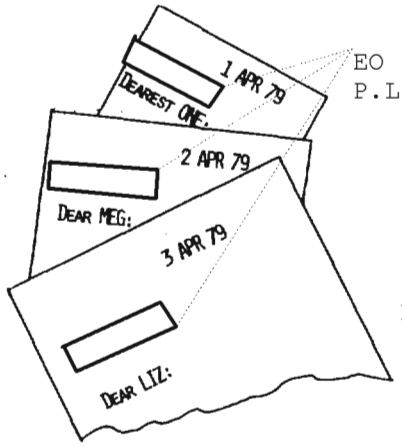
(Continued on page 18)

P.L. 86-36

A Logical Sequel to "A Small Problem"
(CRYPTOLOG, *November 1978*)

A Somewhat Larger Problem (U)

By [redacted] P14
For the Crypto-Traffic Analytic
Special Interest Group



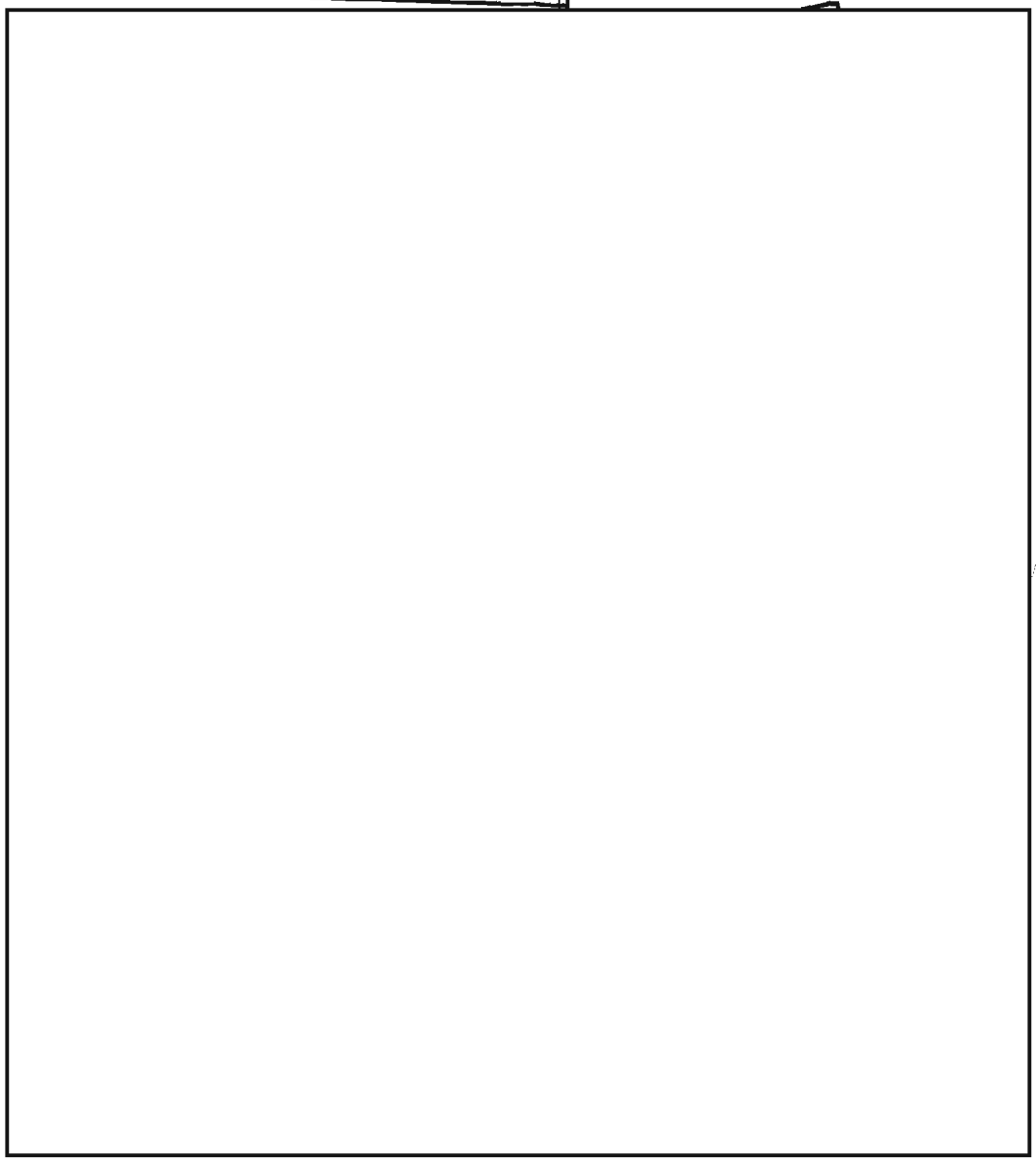
EO 1.4.(c)
P.L. 86-36

EO 1.4.(c)
P.L. 86-36

[redacted]

CLASSIC CABLES (U)

Not as well-known, perhaps, as Murphy's Law, but no less valid, is Hill's Axiom of Cable Analysis: *The exasperation of the cable drafter is directly proportional to the number of reference messages cited.*



FEAR OF TESTING

...and What To Do About It

"Examinations are formidable even to the best prepared, for the greatest fool may ask more than the wisest man can answer." P.L. 86-36
Charles Caleb Colton, 1780-1832

"Tell us your phobias, and we'll tell you what you are afraid of."
Robert Benchley, 1889-1945

Employee testing programs of one form or another have always been a way of life, but in the Age of Professionalization, oral and written professional certification examinations have become key factors in career advancement. At NSA you can't become certified unless you can pass written, and perhaps oral, examinations. Unless you're certified your chances of promotion to the higher grades are drastically reduced. For better or worse, tests are used by management to promote people to positions of greater responsibility (and pay).

Examinations that are fair, relevant, and professionally prepared and administered can be useful tools to help managers determine whether candidates for professionalization have the basic elements of knowledge required for certification by NSA.

But what about those people who are unable to take examinations or give oral presentations because of legitimate irrational fears (phobias)? Fear of test-taking and speechmaking are common phobias, and isn't it likely that the NSA population has some otherwise functionally superior people who are thrown into a deep panic and become truly dysfunctional even at the *thought* of having to give a briefing or take an examination, particularly when the results will significantly influence their career progress?

Most of us know people who have similar fears (heights, flying in airplanes, for instance), but they usually avoid the problem by getting jobs where they aren't required to confront their fear. NSA people who fear tests have no such escape. Their job advancement requires that they make a choice of submitting to tests or remain at a sub-professional level. Because of irrational, pervasive fear (and not because of a lack of subject knowledge or career potential), a number of our coworkers will consistently fail oral and written examinations. Even worse, some people will flatly avoid situations which call for oral or written exams. As a result, these people reconcile themselves to remaining at below-professional grade levels rather than to be subjected to the unbearable (to them) stress of test-taking. They hurt themselves, but they also deprive the government of the benefits of their full potential.

By now some readers may have become impatient with my deferential attitude toward the phobic professional aspirant. After all, didn't most of us have to go through the testing process? Aren't nervousness and apprehension normal side effects of taking the Professional Qualification Examination (PQE)? Am I not just leading up to a plea for special privilege, test waivers, or some such other gimmick which favors people who may be just too lazy or timid to meet the general standards that all professionals have met?

Definitely not! I am attempting to highlight the existence of a real problem at NSA, and to offer some ways for our phobic coworkers, with our help and encouragement, to overcome their fears permanently. No waivers, no special treatment, just an awareness on our part (those of us who can take tests without too much anxiety) that some people do have overwhelming difficulty when confronted by career-related tests; and an understanding by the phobics among us (and they usually know who they are, even if we don't) that they can be permanently relieved of their fears by a variety of proven methods.

To understand the problem let's look at the phobic person. He is usually an otherwise "normal" person who has such an irrational fear of a thing or a situation that he will go to almost any extreme to avoid it. He cannot be cured by pleas, arguments, de-

crees or threats. If a test phobic is forced to submit to an examination his performance will probably be uncharacteristically poor and not a true measure of his knowledge. He may manifest one or more symptoms of panic, such as sweating, upset stomach, breathing difficulties, disorientation, confusion, flight, or avoidance (by just not showing up). It's likely that the phobic person will keep quiet about the problem to disguise the true extent of his difficulty.

What can be done? Quite a bit, since in the vast majority of cases the fear reaction is simply learned behavior.* According to behavior therapists the phobic person has the irrational fear because it was "learned" at some time in the past. By directly treating the phobia symptoms they can be made to go away when they are "unlearned."

Behavior modification therapy for phobias does not require that the subject acquire an insight into how or when the phobia began. Treatment generally does not involve in-depth analysis of inner forces, deeper psychological problems, and the like. Therapy usually consists of simple techniques which are designed to unlearn the anxious behavior associated with the phobia, and can involve procedures called *modeling* and *desensitization*. *Modeling* assumes that the phobia may have been learned from observing others who exhibited anxieties in stress situations (perhaps how my friend in the footnote helped to learn his fear of flying). The unlearning process involves observing others while they display fearlessness in the threatening situation. *Desensitization* is a procedure which uses relaxation, thought-stopping and other methods to systematically reduce sensitivity to the anxiety-causing situation. During desensitization sessions the subject visualizes various situations in his or her "anxiety hierarchy," which are typically imagined situations that have progressively disturbing reactions.**

* A friend of mine has refused to fly ever since an encounter with violent air turbulence. He relates that while dodging flying dishes he looked to the flight attendant for some sign of strength and calm. He vividly recalls that she appeared more terrified than most others on the flight. The lesson of the day was fear, and my friend learned his lesson well. He has not flown since, but perhaps after reading this article he will have a go at some form of phobia-fix and become a flying fool.

**Typical situations you might visualize if you had test-taking fears might be: "You hear about someone who has a test" (low anxiety); "You are in an important exam. The instructor announces that 15 minutes remain, but you have an hour's work left" (high anxiety).

Using special techniques the subject gradually unlearns the phobia symptoms and is then free to function normally, usually within a surprisingly short time. Thankfully, phobia patients are not generally subjected to cold-turkey "cures" like: "OK, everybody onto the airplane," or "give us a 15-minute speech."

Behavior therapy for phobias really works. Even people who feel that *they* will *never* be cured, find that they can usually unlearn the problem symptoms and can then face the phobia situation with confidence. Since the behavior therapy approach to phobias makes no judgments about the mental health of the subject, but treats the phobia as essentially a bad habit, phobic subjects who might otherwise have an aversion to psychological and psychiatric therapy need have no qualms about undergoing simple behavior habit modification treatment.

There are several methods available to people who want to get a phobia problem resolved, particularly one which is associated with NSA work situations like the PQE. These include consulation with M72 clinical psychologists, outside private therapists (no NSA knowledge or involvement), or do-it-yourself techniques. I'll examine each of these methods and give some idea of how to go about getting assistance for yourself or advising someone you know on how to get help.

One way in which an NSA person can seek professional assistance for a phobia is through M72 Psychological Services. I spoke with Dr. [redacted] Chief of M72, and his staff about phobia treatment for NSA employees. They confirmed that they have encountered a broad range of phobias among NSA people, and occasionally, NSA family members (for example, a family member has a fear of flying which prevents the employee from accepting an overseas assignment involving air travel). P.L. 86-36

Although the M72 psychologists are prohibited by statute from conducting long-term therapy, they do hold a limited number of sessions with the patient to determine that the problem is a true simple phobia. After diagnosing a phobia (rather than a more complex problem of which the phobic symptoms are only a smaller part), they will provide the employee with a list of four or five private practitioners who are known to be legitimate, effective phobia therapists. The employee selects his or her own professional and makes private arrangements for treatment. Cost is borne by the patient, generally with the financial assistance of major medical insurance carriers. The Columbia Medical Plan reportedly also has a program for treating phobias and the M72 counselors can provide more specifics, or CMP members can make arrangements on their own.

Once the patient makes contact with a therapist the treatment could involve indi-

vidual or group sessions. For the more specific and common phobias treatment is often short-term, and frequently successful.

The M72 staff stressed that they maintain anonymity and confidentiality for self-referred phobia subjects, and there need be no official NSA awareness of the transaction. They pointed out that the Baltimore-Washington area has an impressive array of top-rated phobia therapists and that help is often readily available and effective. For an appointment with an M72 counselor call 5429s or 6531b.

Another method of obtaining help is by direct contact with a therapist, perhaps on the basis or recommendations from friends or a family physician. Costs vary and are the direct result of patient-therapist discussion. Medical insurance coverage should be checked before beginning therapy to make sure of what the insurance carrier will provide.

Those who prefer to arrange their own therapy might be interested in the Johns Hopkins Behavioral Medicine Clinic in Baltimore, which is a private clinic dealing in the treatment of phobias. I spoke with the Clinical Director, Dr. Bruce Masek, who gave me some useful information on what would be involved in obtaining treatment. The clinic treats all major phobias, using behavior modification. Patients are also given individually prepared cassette tapes to take home and supplement the formal desensitization sessions. Visits cost $50 per hour, some of which may be covered by major medical insurance (check first).

Dr. Masek suggests that interested patients first call the clinic (955-6111) to discuss with a staff member the nature of the phobia and to arrange for a visit to the clinic.

Do-It-Yourself Phobia Fix-up. If you have a common phobia which is either directly or indirectly influencing your career you can take personal control of the situation and probably cure the phobia yourself. This can be done with the help of inexpensive books and cassette tapes which are broadly available. These materials are usually written in simple, non-technical style and generally use behavior modification techniques to enable the serious reader to systematically break the phobia habit. These books and tapes can be very effective aids to people who are serious about breaking the hold of a phobia on their lives. A short listing of some typical books and cassettes is included at the end of this article. If self-treatment is for you, then you should check out these inexpensive materials.

Test-Taking Strategy. Since tests have become so important to NSA career advancement, what can be done for the person who doesn't necessarily have a phobia, but who hasn't learned how to organize and make the best use of time, strategy, briefing aids and techniques, and the like, when taking written or oral examinations? He or she knows the test material, has no overwhelming anxiety, but bogs down in the mechanics of the test-taking procedures and does not play the odds properly, or does not handle the mechanics and style of an oral examination in a convincing way.

The goal of testing is to assess the knowledge or skill of the testee without imposing arbitrary test-related barriers. In the case of professionalization tests which have a direct influence on the careers of our employees, the Agency has a responsibility to make the test procedures as neutral and transparent as is possible. People aren't supposed to be tested on their ability to survive tests, but on their knowledge of the material.

In 1974 the Women in NSA (WIN) organization conducted a lecture on How to Take Exams, but it was oriented more toward the general CQB and proficiency tests. Something similar but on a more intensive scale needs to be offered periodically for prospective professionalization aspirants. Both written and oral examinations should be covered in the sessions, which could be available to all who may want or need assistance.

Prospects for Change. As certified professionals, managers, and coworkers we should satisfy ourselves that no arbitrary (even if unintentional) test-related career roadblocks are place in the way of *any* aspirants to professional certification.

If our subordinates are failing or avoiding tests or special work situations because of irrational fear, it is our responsibility to work with them to see that they resolve the problem. The professionalization panels should make it their business to know their aspirants well enough to detect likely test-avoiders, and get to them with the facts about how to seek help.

It will be very difficult for us to determine exactly how many people are dodging or consistently failing professionalization tests because of irrational fear. Test fearers are less then enthusiastic about publicly declaring their fears,* and would also seem to be

* One NSA person I talked with (a proven excellent worker, but a test fearer) went *years* before being able to successfully survive the PQE in his field. During these years he downplayed his fear of tests because he felt that management would interpret his phobia as a general inability to function under *any* stressful situation.

generally disinclined to present themselves to the NSA Medical Center for psychological counseling. The situation is further complicated by the federal prohibition that government agencies may not engage in extended civilian medical or psychological therapy, since this is legally and logically the province of the private sector. Our military SCA associates have have an even stronger reason to avoid treatment for phobias. Many believe that if they were to seek assistance for a phobia their authorization for access to classified material would be pulled immediately, on the grounds that any contact with mental health professionals connotes a potential security risk.

If we are really to come to grips with the issue, active measures can be taken on behalf of our people, many of whom cannot afford private therapy. One possible solution could involve contracting for private practitioners to come to NSA and present periodic "How to Take Tests and Be Comfortable While Doing It" sessions. Technically, behavior modification is training (or more accurately, *re*training) and makes no judgments about the psychological health of the subject. It could follow that NSA-sponsored special retraining sessions would be legal and ethical endeavors.

Another possibility would be for the NSA Learned Associations (The Collection Association, The Communications Analysis Association, etc.) to sponsor and fund "How to Take Tests" seminars conducted by qualified outside consultants. These sessions could cover the mechanics of oral and written test-taking and testing strategy, and could also offer, for those who are interested, some basic information about how to deal with the various forms of test anxiety. At the least, a session entitled "How to Do Your Best in Professionalization Tests" has a better chance of getting to the people who need it than for us to expect all of them to come forward and admit a "phobia." Self-help books and tapes should be made broadly available by the Professionalization Panels and Learning Centers. Remember, most of the true phobics have long ago decided to accept their present position and grade rather than face the anxiety of even *visualizing* themselves in the feared examination situation. It's up to us as friends (and managers) to give them the support and help they need to solve their own problems. Strictly speaking, any employment procedures or testing mechanisms that operate as "built-in headwinds" to any class or group of people (in this case, phobics) could be unlawful, even if there was good intent or absence of discriminatory intent on the part of the government. When you think about it, if just one gifted person can be helped to overcome his or her fears to the extent that our tests will measure only ability and knowledge, we will have done a good thing.

In his address to the Communications Analysis Association on 10 May 1978, the Director, VADM B.R. Inman, very candidly spoke of his concern that the Professionalization process might be in need of a more sympathetic and less bureaucratic view by the Agency.

> I am struck that there is often a very *bureaucratic* approach to professionalization, and, demonstrating my relative ignorance, I have a sense that maybe the Agency as an organization doesn't do all it could to facilitate that professionalization process, to make it easier to help put the things together that can help you get through those hurdles. I believe there are clearly improvements that can be made."

The Director's comments, while not specificially addressed to professionalization testing, nonetheless give us the support and emphasis we need to size, attack, and solve the problem of test fear at NSA.

Let's get started.

SELF-HELP MATERIALS

The following are typical of the broad range of self-improvement books and tapes available to help people with irrational fears. I make no claims as to their effectiveness, but they are representative of what's available.

Nothing to Fear, Fraser Kent (Dell, $1.95). Explores various approaches which can be applied to self-cure of phobias. Uses simple layman's language.

Fear: Learning to Cope, Albert G Forgione and Richard S. Surivit, with Daniel G. Page (Van Nostrand Reinhold, $9.95). A specific guide for dealing with phobia, using all the modern therapeutic techniques. Considered an easy-to-follow guide. These authors have developed a successful program for flight phobia.

Stop Running Scared! Herbert Fensterheim and Jean Baer (Dell, $2.25). Oriented toward the do-it-yourselfer, with step-by-step plans to overcome most fears. Includes a proven learning plan to help conquer fear of flying. Contains instructions for preparing a personalized relaxation tape.

Kicking the Fear Habit, Manuel J. Smith (Bantam, $1.95). Written for the do-it-yourselfer. The author claims that using his method of therapy can often lead to rapid conquering of chronic fears.

Phobia Free: How to Fight Your Feare, E. Ann Sutherland and Zalman Amit, with Andrew Weiner (Jove/HBJ, $1.95).

Phobia Free and Flying High, Neal H. Olshan with Julie Dreyer Wang (Condor, $2.25). Offers step-by-step procedures to help the reader identify and eliminate phobias.

Casettes are available from Psychology Today Cassettes, P.O.Box 278, Pratt Station, Brooklyn, N.Y. 11205. A free catalog is available and subjects include "Deep Relaxation" (#20040) and "Getting Rid of Your Fears" (#20155), at $8.95 each. The latter tape is by Manuel Smith, author of *Kicking the Fear Habit* (above), and reportedly explains how to cure phobias such as fear of flying, heights, taking tests, etc.

more Fairbanks on English

Last Month CRYPTOLOG *reprinted a 1958 editorial written by Dr. Sydney Fairbanks when he was at the helm of the* NSA Technical Journal, *on the subject of NSA English. The response to this was sufficiently encouraging as to warrant trying it again. Here, from the issues of January and April 1958, are two more of Dr. Fairbanks' comments on this subject.*

We promised last time to write a series of notes on the grosser abuses of the language to which the job exposes us. Our text for today will be the curious locution "this type thing." No one says, we believe, "variety thing," or "sort thing," and there is a natural bar against saying "kind thing" (consider, for instance, "I hate your kind letter."), so that this cannot be a mere extension of a Milt Gross idiom ("With your pie you want it a piece cheese?") nor an offshoot of the sort of telegraphese that omits all connectives ("Reference your message"). We think the main culprit is the technical writer.

An English epigram which is still going the rounds—last seen in *Missiles and Rockets* —defines an engineer as a man who says "a coffee-containing cup" when he means "a cup containing coffee." If, one may add, he wishes to talk about a description of the methods used in teaching the design of gadgets to be used on widgets, he will write "a widget-type gadget design instruction methods description." We have had the equivalent of this submitted to us for publication. As for writing "widget-type gadget" rather than "widget type of gadget," he does it every time. It is, after all, not incorrect though a trifle monotonous. And since he has little use for hyphens, he writes "widget type gadget." From this some illiterate soon concludes that "type" *means* "type of," and the step to "this type thing" is immediate. Since it is well known that no error is stupid or vulgar enough to guarantee that it will not become respectable, we refrain from rending our garments. But we submit that at this period English this type writing is not appropriate to this sort Journal.

And so to bed.

* *

No violent protests having been received, we continue our remarks on how not to write English. A sentence—suitably disguised, we trust—in a recent contribution, runs something like: "The machine has the power of selecting the ripe apples and throw away the others." Most readers will conclude that the typist forgot to type an "ing", and so what. But our calling has made us so suspicious that we are inclined to see in this a first seeping into written English of something that is rapidly becoming a standard colloquialism. Observe its history. The verb "to go" has two functions in English— one to express the future: "I am going to do what he asks"; and another to express motion: "Where are you going?" Another way of expressing the future is by using the continuous present: "I am driving out there tomorrow." Out of a horrid amalgam of these has grown up the very common, but indefensible, "I am going upstairs and take a nap," meaning "I am going to go upstairs and take a nap" or "I am going upstairs to take a nap" or even, "I am going upstairs (this afternoon) and taking a nap." But there is no use in trying to make a chart of chaos.

Even though "I am take a nap" and "I am going take a nap" are both very queer, it might be possible to put a fence around the monster and say, "This is something peculiar that happens with the verb 'to go'." But alas, the spirit of the language is never more logical than in extending its mistakes. If Momma is going upstairs and take a nap, what is more natural than that if Willie disturbs her she is coming downstairs and beat his ears in, or than she is running through her mail and throw the advertisements in the trash, or taking a bus downtown and buy a hat, or for that matter joining the Navy and see the world.

A reader told us recently that on encountering our remarks about "this type thing" he couldn't imagine what we were talking about; never in his life had he heard anybody say anything like that; but that in the next twenty-four hours he had heard it four times. In the same spirit we direct the attention of our word-watchers to this new idiom that is creeping into the language and poison our intellects. There is no sense in temporizing and let it get established. It...

Ugh!

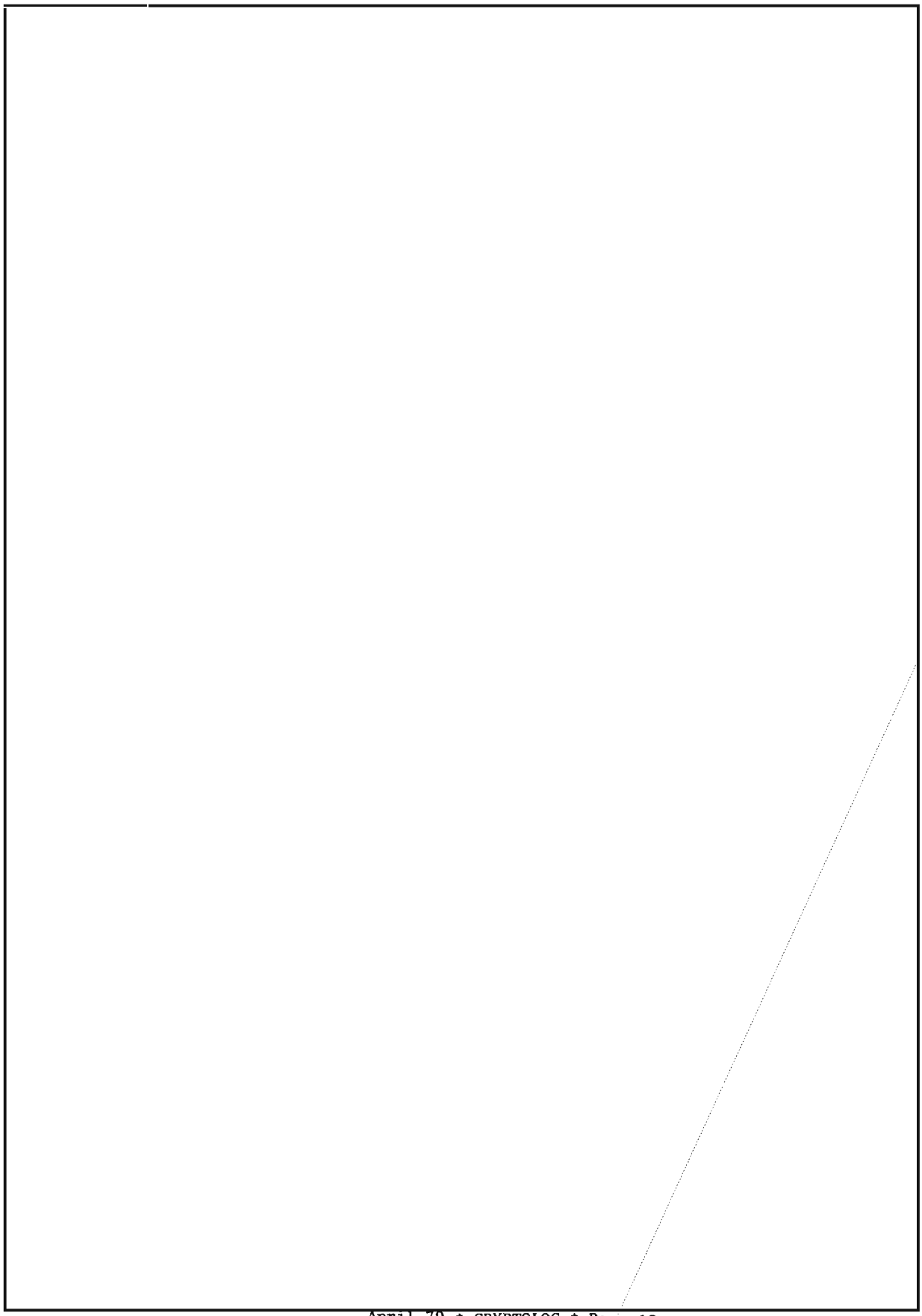
NSA-crostic No. 24 (U)

By D.H.W.

The quotation on the next page was taken from a published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS

WORDS



LETTERS

To the Editor, CRYPTOLOG:

I would like both to support and state my appreciation of Mr. Gurin's article, "Let's Not Forget Our Cryptologic Mission," which appeared in the February issue of CRYPTOLOG. I would like to point out an oversight I believe Mr. Gurin made, but first I must state that I heartily agree with his remarks about the ratio of jobs totally involved with the Agency's basic mission to the ever-increasing number of jobs which have only an indirect impact on that mission. My particular COSC (1640 series, Collection), according to the most recent Quarterly Management Review, is said to be near its authorized strength. But we must really look behind those figures, and see how many people who carry a 1640 series COSC are actually involved in the collection effort. If we are near our authorized strength, why is it that so many collection jobs are unfilled at many of our overseas locations and in the ROFs (Remote Operating Facilities) here at home? The job description and grade span stated in the PMM shows that a collector can go as high as a grade 12, but in reality, I would be hard pressed to find any grade 12s actually doing the collection effort. This point is stressed because it underlines Mr. Gurin's feeling that we are getting away from our prime mission in many areas.

The oversight I would like to mention concerns Mr. Gurin's numbering scheme as it relates to the basic mission of the Agency. If Mr. Gurin's system is applied and the TA people, the cryptanalysts, appropriate program managers, and so forth, are given the rating of 1, where does that put the collection personnel? Have we forgotten that the person who gets the ball rolling, provides the raw material for the finished product, the person who takes the first step in the long, long journey, is the person who performs the most basic, and in some people's opinion, the most important part—the collector?

[redacted]

Jack Gurin responds: [redacted] has caught me dead to rights. What could be closer to the basic mission than collection? In my own defense, though, I should say that I was not trying to provide an exhaustive list, just a sample to illustrate the point. Perhaps what I should have done would have been to visualize how one would start all over again to build a cryptologic agency, and list what kinds of people would have to be hired. I sure wouldn't have missed the collector.

To the Editor, CRYPTOLOG:

I'm sorry that the "Ask Art" column you had in December's issue was a one-time thing, because I have a problem and I need HELP.

I'm trying to fill out all of those forms you get when you're updating your personal history statement for security reinvestigation. One form in the packet calls for full maiden names for my mother and my spouse. Mother is no problem, but, as far as my spouse is concerned, even after umpty-zip years of marriage, he still refuses to tell me his full maiden name.

What shall I do?

Sue

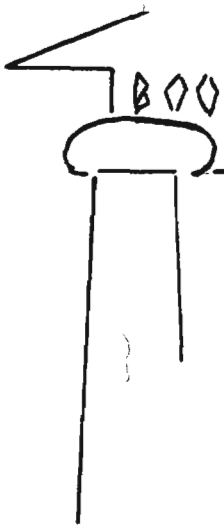
SOLUTION TO NSA-CROSTIC NO. 23
(*CRYPTOLOG*, March 1979, by A.J.S.)

[redacted] "[Tell Me I'm Just a] Sinobibliophobe!", *CRYPTOLOG*, July 1978

"If any significant number of those worker-peasant-soldier students self-studied their way through that [Chinese mathematics] textbook, the present technological advantage of the United States (and of the USSR) might not remain so overwhelming all through the foreseeable future."

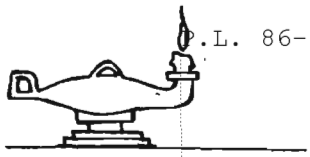
NEW EMPLOYEE?
JUST BEEN TRANSFERRED??
JUST BEEN REORGANIZED???

To start a new subscription to CRYPTOLOG, or to change your address on an old one, call the CRYPTOLOG office. The phone is 3957s.



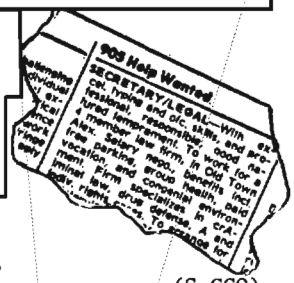
BOOKBREAKING BRIEFS (U)

~~(C-CCO)~~ NCS FELLOWSHIP. The National Cryptologic School is announcing a Cryptologic Education Fellowship to update the course in code reconstruction and to teach it the first time. The present course is based on codes and techniques—and administrative philosophy—that were current in the early 1950s, but updated from time to time since then. Now an overhaul is needed to integrate these piecemeal updates; developments in computer technology and changes in target codes compel it. The new course, like the present one, will allow for guest lecturers to address the class on specialized topics. The selectee will work with member(s) of the Analysis, Design, and Development Department to insure that the course incorporates, where feasible, the latest techniques in instructional technology. The Cryptanalysis Division offers assistance on content. The facilities of the Bookbreakers' Forum will be available to the selectee. Applicants should be experienced bookbreakers conversant with modern bookbreaking techniques and knowledgeable in the theory and principles of code reconstruction. Applications should be submitted through channels to M02. For further information, call [redacted] Chief, E42, 8025s.



P.L. 86-36

[redacted]



Is there a better way? If you know of one, or have such a problem, come to a workshop meeting of the Forum on Tuesday, 24 April at 0930, in Room 2C078. If you'd like to talk about the problem in advance, call [redacted] on 5236s or 5642s. ~~(S-CCO)~~

CLARIFICATION (U)

Classified ~~SECRET-UMCCO~~ in entirety

The January 1979 issue of CRYPTOLOG carried an article in the Classification Corner concerning classifications of references to Second and Third Parties. One point made in the article apparently needs clarification, since we have received several inquiries concerning its intent and meaning.

The article stated that "references to 'Second Party' or 'Third Party' which are made in a COMSEC context, whether stated or implied," are unclassified. The intention was that the term *second party* (not the specific country) would be unclassified when so referenced.

Revealing a COMSEC association between NSA or the U. S. and a *specific* Second Party country or organization without amplification is classified as follows:

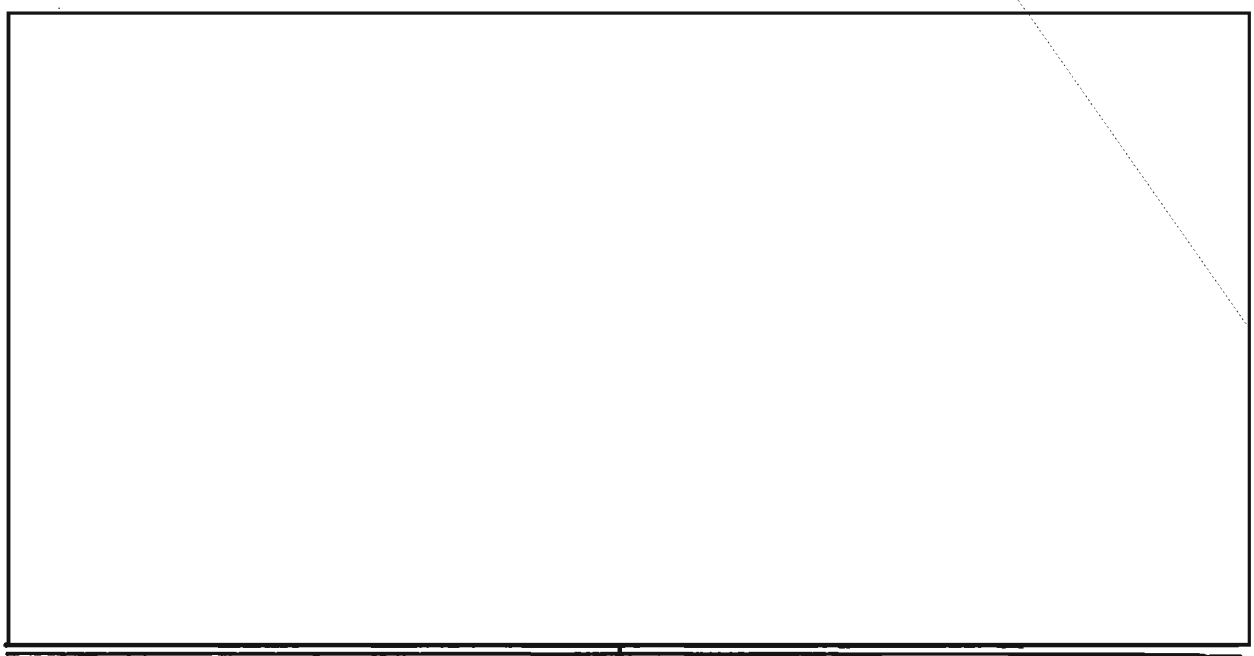
EO 1.4.(c)
P.L. 86-36

with GCHQ or the UK: Unclassified
with CSE or Canada: Unclassified

[redacted]

When classifying a Second Party relationship, be mindful of the fact that the minimum classification of [redacted]

P.L. 86-36



Following his talk, Mr. Boak answered questions from the floor. (This portion is classified ~~CONFIDENTIAL~~ in entirety.)

Q. What are your views on the extension of cryptography in the public sector and the initiatives of the Department of Commerce?

A. Frankly, I'm not overly concerned. I think some of us may have overreacted to the surge of activity out there and some of the publicity we got with respect to it. I think most of my SIGINT friends now believe that it is not going to be the end of the world. Clearly, though, as more and more sophisticated knowledge about cryptography is proliferated in public, it is going to make the SIGINT job harder, and take more people and other assets to sustain our present level of success. But the consensus I see is that the problem is not an insuperable one.

EO 1.4.(c)
P.L. 86-36

The ascendency of the Department of Commerce in this field resulted from a presidential directive which established *two* Executive Agents in the government for telecommunications protection: one which has to do with the protection of national security related information—this is NSA, acting for the Secretary of Defense, and one for the protection of information not related to national security—this is the Department of Commerce.

The action element in Commerce is a new organization, the National Telecommunications and Information Administration, with whom we are now in active negotiation on how to share this load. We have some concerns, of course. Are they, for example going to create an independent cryptanalytic organization? Are they going to do independent R & D in cryptography? And if so, under what kinds of security controls?

Overall, however, we are becoming acclimated to one another and the Director is ensuring that we remain highly cooperative and supportive of them.

Q. Do you anticipate that the S organization will establish a viable ELINT security (ELSEC) program?

A. We have wrestled with that matter for as long as I've been around. We have not solved it. For a while, we thought of calling ourselves "SIGSEC" instead of COMSEC, thus solving the issue with improved nomenclature.

But it is true that we have no coherent ELSEC effort because we have been unable to define it very well. Yet those definitions are important in establishing roles, missions and authorities.

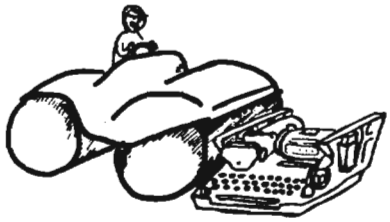
[redacted]

Q. Will NSA establish a national COMSEC assessment program for equipment other than that we build ourselves?

A. I hope not. It's a very difficult thing. If some of the equipment being produced commercially is going to be adopted by elements of the government, I believe we must have some role in its certification or validation. But I believe the way we go about that, if the equipment is not to be used for national security purposes, will have to be through the Department of Commerce, as their new mission gives them jurisdiction over such applications. We will offer them technical advice and assistance on how good such systems are.

[redacted]

BUT, MR. BOAK, DID YOU EVER TRY TO GET RID OF ONE IN A HURRY! (U)



By D.H.W.

(U) Dave Boak has stressed the cryptographic integrity of the cipher devices produced by S. But there is another, quite different, aspect of the superior quality of these machines which he didn't cover, which I'd like to touch upon. That is their structural integrity.

(U) Cipher devices, like most other DoD equipment designed for use in the field, are manufactured in accordance with something called military specifications—milspecs, for short. One of the features of manufacture which milspecs cover is ruggedness. For example, some items designed for the Army and the Air Force must be capable of operating in the severest of climatic conditions, from Saharan to Arctic, while many items intended for shipboard use by the Navy must be able to operate under temporary conditions of flooding.

(U) On the other hand, cipher equipment, *unlike* most other DoD hardware, is classified. This means that at field locations where there is a risk of loss for whatever reason, the station commander and the crypto custodian must be prepared to destroy the commcenter gear, often on short notice.

~~(C)~~ Now it's readily obvious that milspec-imposed ruggedness and ease of rapid destructability are somewhat at odds. Something has to give. And the clear winner, at least as far as two of the most popular devices in the S inventory are concerned—the KW-26 and the KG-13—is milspecs.

~~(C)~~ A few years ago I was involved in the [redacted] From one day to the next there was no particular hazard, so we stayed on, packing and shipping back much of the station equipment. But since there was no

way of predicting what might happen a couple of days in the future, I got a bit edgy about the crypto gear. I didn't want it sitting around somewhere for days at a time waiting for pickup by ARFCOS (Armed Forces Courier Service) or by diplomatic courier. So I sent a message back to S requesting permission to destroy the classified portions of this equipment.

(U) Now they don't fool around in S. When it comes to balancing dollar costs against crypto security, it's no contest. Of all the requests for guidance I sent to NSA during this period, this one drew the fastest reply: if you feel there's any risk of loss—destroy.

(U) Emergency destruction plans envision more than one type of emergency, depending on urgency. The most critical is they're-breaking-down-the-front-door right-now, which involves destroying everything in its installed position. Some of our more adventuresome people wanted to try this, but since it would have, at the very least, rendered our operations building uninhabitable for some time (and at worst, burned it to the ground), we rejected this approach, taking a more leisurely one.

(U) All the classified devices were removed from their racks, carried outdoors, and laid out on the ground. Next we put a destruction device on each one.

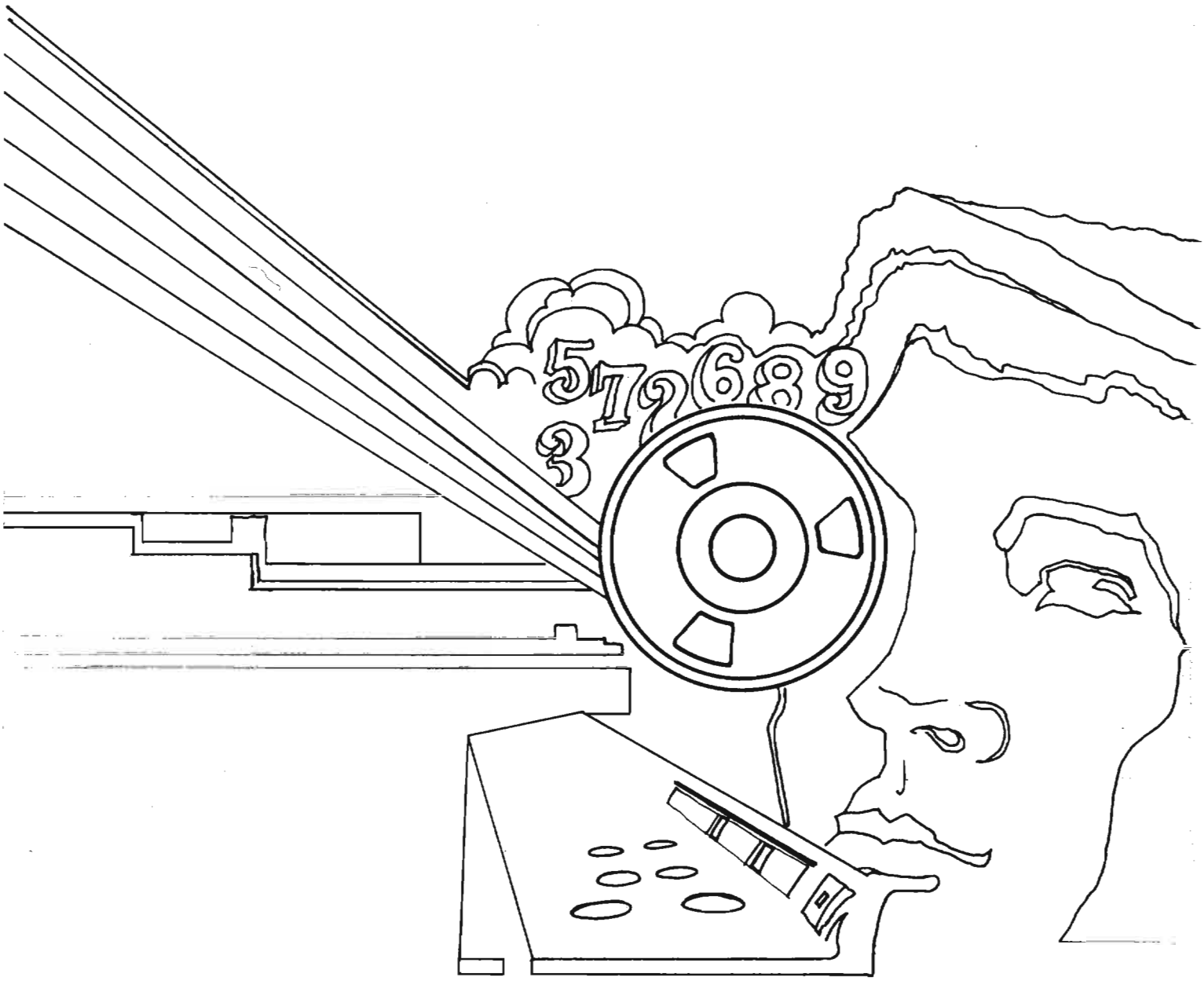
(U) The first thing that became apparent was the wisdom of not performing the destruction indoors. A towering column of thick black smoke rose straight up hundreds of feet in the air, while the heat given off caused us to step further and further back. After a minute or two I went inside and called the two other local U. S. installations (the Consulate General and the Naval Communications Unit) to advise them that we were neither under attack or burning down, that the smoke column was perfectly routine.

(U) CLA — NCS FOREIGN FILMS FOR SPRING (U)

Thursday, 26 April, 1300 hours: "The Hero's Wife" (Hebrew)
Tuesday, 1 May, 0900 hours: "Italiano Brava Gente" (Italian, German and Russian)
Thursday, 31 May, 0930 hours: "True Friends" (Russian)

IN THE FRIEDMAN AUDITORIUM

E.O. 1.4.(c)
P.L. 86-36


5 7 2 6 8 9
3