~~TOP SECRET~~ 980

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

[redacted]

TOLOG

P.L. 86-36

MAY 1975

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA (NSAM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

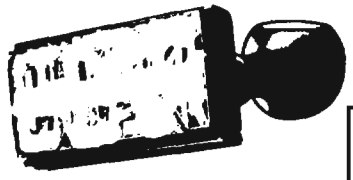
VOL. II, NO. 5 MAY 1975

PUBLISHER WILLIAM LUTWINIAK

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

~~TOP SECRET~~

"CODEWORD" OR "COMINT CHANNELS"?



P.L. 86-36

[redacted]

V1

To the average person, the words ΑΚΡΩΣ ΑΠΟΡΡΗΤΟΝ, ΑΠΟΡΡΗΤΟΝ, and ΕΜΠΙΣΤΕΤΙΚΟΝ are just three Greek terms. Translated, these terms are TOP SECRET, SECRET, and CONFIDENTIAL, but unfortunately, to many NSAers they are still Greek. We in NSA know how to handle papers and documents with the various classifications affixed; our problem is in determining the classification of papers that we ourselves originate.

One of the major classification difficulties is determining whether certain information belongs in a COMINT category (that is, requires a Codeword on each page) or whether it must merely be kept in COMINT channels.

The definition of "COMINT Codeword" is information that, if compromised, could cause damage to national security, and specifically to COMINT activities. (Any paper, for instance, that quotes a COMINT source, directly or indirectly, requires a Codeword because it reveals that we are successfully reading certain traffic--information that, if compromised, would certainly jeopardize that traffic.) Such information requires handling that affords the highest degree of security protection. Of course there are various degrees of damage and of protection, depending on whether it is COMINT Category I, II, or III.

"COMINT Channels" information is that which, though less revealing, must still be limited to COMINT-cleared personnel because it contains information related to COMINT agencies or activities.

To aid in determining which group our paper falls in, we can look at the rules and guidance in the NSA/CSS Classification Manual and USSID 3. These guidelines often provide just the information we need. However, when we cannot find a specific rule or guide to solve our classification problem, we must use the general definitions and good old-fashioned judgment. Some hints in the judgment area are:

Very sensitive SIGINT plans and operations sometimes require greater protection and carry a COMINT Codeword classification just for that reason.

If the document reveals a degree of success or progress in the production of COMINT or a sophisticated COMINT technique, a greater protection than "COMINT Channels Only" is required.

Information classified by another agency or government may carry a higher classification than that we would have used, but we are required to apply the same classification as the originator.

As a Classification Advisory Officer, I am often called upon to assist in determining whether certain information is "Codeword" or "COMINT Channels." It is not always a clear and easy decision. I use all of the available guidelines and judgment factors mentioned above. When this does not give me the proper classification, I approach the problem in another way. I work on the supposition that the material I am trying to classify is compromised and falls into the hands of the enemy. With this information, what countermeasures can he (the enemy) take to insure that such information will not be available to NSA again?

If the exact time, date, place, and means of acquisition are available from the information, he can take extensive measures to insure that such information will not be communicated in the same manner again. He can change call-sign systems, frequency systems, schedules, and cryptosystems, and impose strict limitations on chatter usage, and he can do so at a particular transmission site. When your information fulfills some or all of the criteria above, it can easily be determined to be "Codeword."

On the other hand, if the paper gives general information related to the COMINT effort but does not include specifics of a transmission or actual transmission procedures or give the enemy information leading to specific countermeasures, it requires only "COMINT Channels" protection.

This can be amplified by way of example. The following problems are fictitious and are used for illustration only:

Mr. Charles Great is recommended for the Meritorious Civilian Service Award for his outstanding achievements while assigned to the National Security Agency/Central Security Service from December 6, 1970 to December 9, 1974. During this time he worked

[redacted] He guided the field sites in their collection efforts and was very helpful in solving problems that existed in their processing and reporting efforts.

This is obviously "COMINT Channels." It tells the enemy that we intercepted, processed, and reported [redacted]

[redacted]

This is obviously "Codeword." It identifies a unit which sent a message on 15 December, and relates the text of the message. [redacted]

[redacted]

[redacted]

~~(TOP SECRET UMBRA)~~

TA, HANDMAIDEN OF CA

FREDERIC O. MASON, JR., P11

Traffic analysis was created, as an analytic function, in order to organize collection and to maintain continuity for support of cryptanalysis. In a broad sense it still does that, but it has also achieved a value of its own,

Before TA was fragmented into many career fields (for reasons which escape me) it was everything in COMINT which wasn't CA, or--more properly--it was a subset of CA, employing many CA techniques, but against a different body of data.

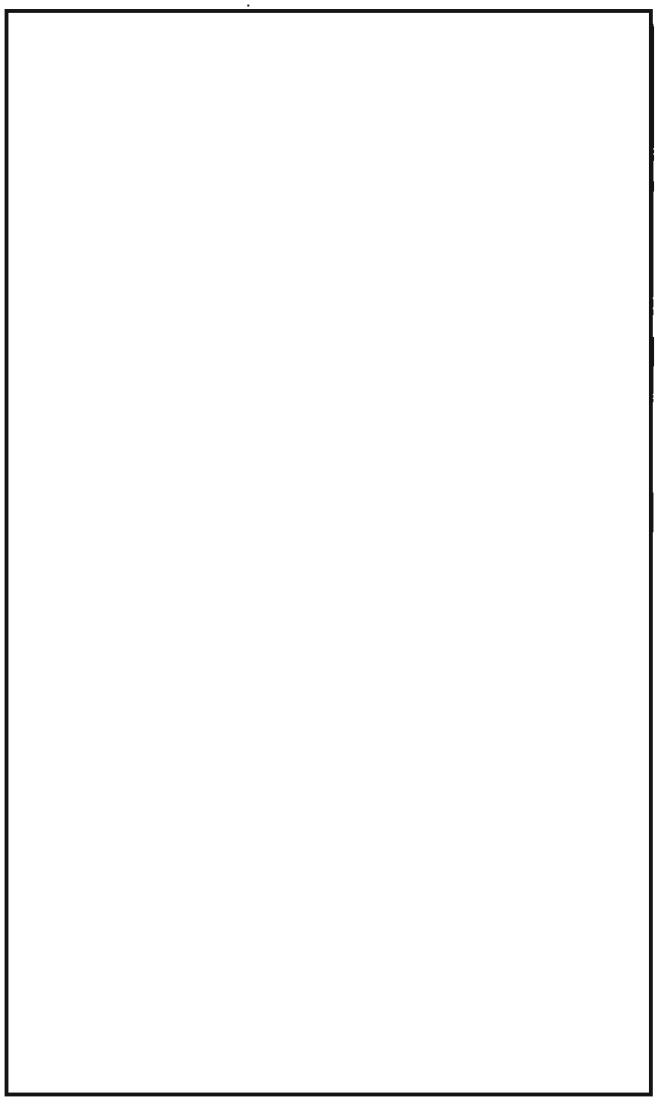
The essential differences between CA and TA are twofold:

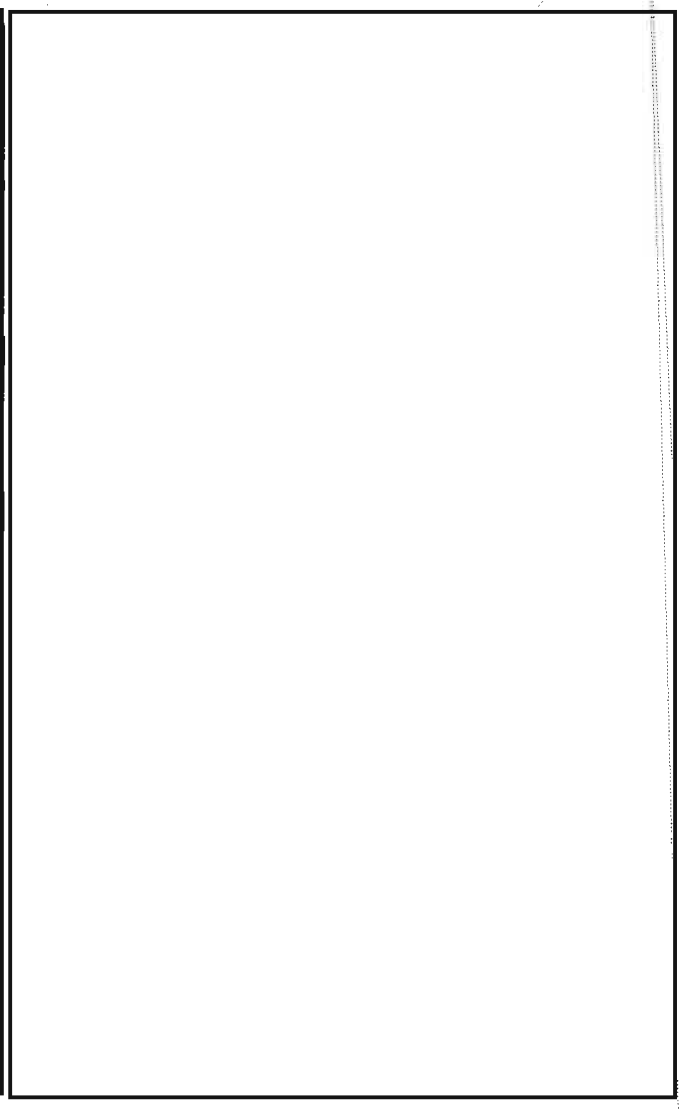
Generally the two skills are inversely important: if CA is very successful, TA is apt to be little valued (though very complete); if CA is stymied, then any TA achievement is valued highly.

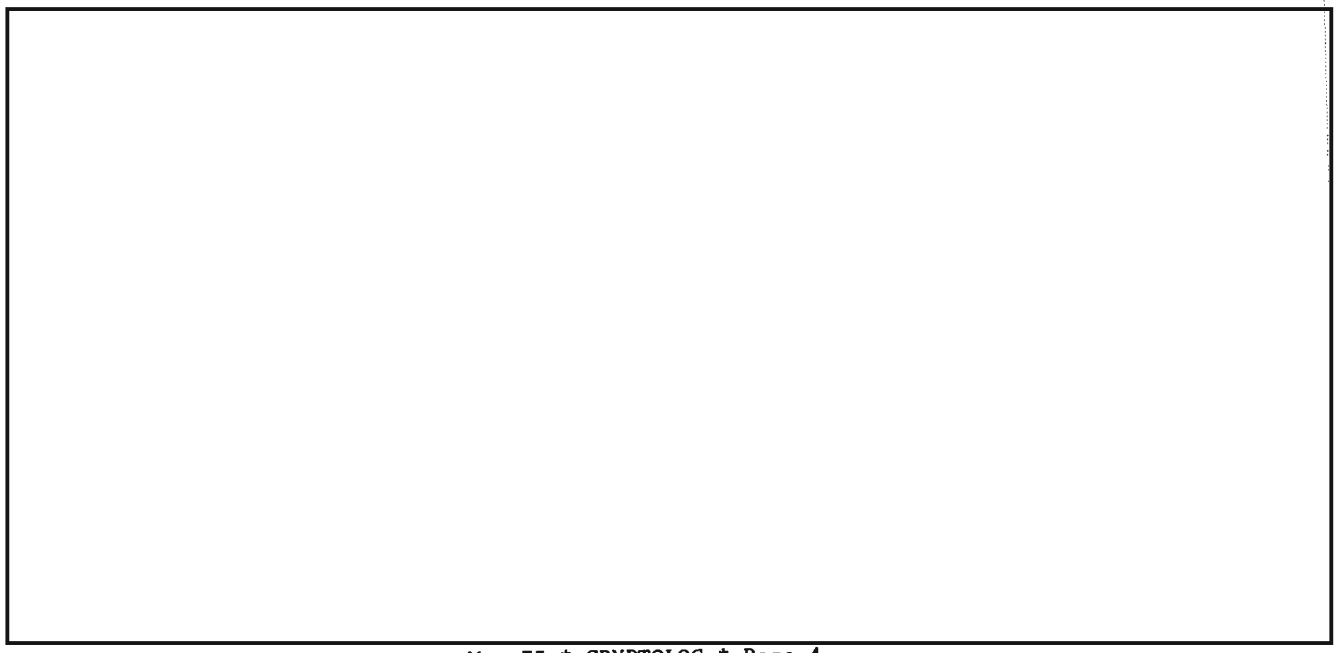
In practice the line between the two is not sharp, since TA normally does many "trivial" cryptanalytic jobs

TA and CA are, then, both similar and interdependent.

~~TOP SECRET UMBRA~~







~~TOP SECRET UMBRA~~

[redacted]

[redacted]

[redacted]

** ** ** **

If this sort of exercise entertains you, we can do some more. Let us know.

★★★ HOORAY FOR PMD'S! ★★★

[redacted] M09

My first impression of Program Management Directives was that the whole process placed an inappropriate emphasis on planning. As a result there appeared to be undue staff involvement in things that had previously been the exclusive domain of line organizations.

More recent experience with a specific PMD dealing with the phaseout of an overseas site changed my views radically.

The draft PMD was given to me with a note saying, "I can see considerable M involvement." My immediate reaction was,"To close out a site? You've got to be kidding!" After a discussion with the Program Manager, however, several things began to come into better focus.

First, the Program Manager asked for an inventory of equipment to include current value, size (in cubic feet), and weight. He indicated that he needed this information to develop an emergency evacuation plan. He had already dispatched crates for key items which were quickly identifiable as worthy of evacuation in a "one-week notice" situation. His plan was to order a sufficient number of C130 cargo planes to the site to accomplish the evacuation in an orderly fashion. He stated that each item identified on the inventory as worth over $1,000 would be brought out in a "one-week notice" situation, and he wanted disposition instructions for this equipment listed with the inventory. He indicated that the instructions need not be "Return to NSAW," since the same equipment might be in demand at other overseas sites being augmented to assume the missions from the phased-out site. The axiom *Planning is Managing* began to surface in my consciousness.

The discussion then turned to the PMD, which was due to be approved in approximately six weeks. The Program Manager stated that he wanted the M input to include time-phased actions as required in the recent revision of NSA Directive 25-3. We began to discuss the implications of a phasing-out mode: the effect of reducing the amount of operations space as systems are taken off line, and the impact of this on guards and alarm systems. It was becoming apparent that there *was* going to be "considerable M involvement."

On the subject of personnel, the Program Manager indicated that ten NSA civilians are currently assigned to the station in addition to the contractor personnel. It struck me that some of those people may be due for rotation back to NSAW prior to June 1976. If so, will they be replaced? Will they be extended? If they are replaced, where will the replacements be sent in June 1976? Then the thoughts came, what about militarizing those billets (M2)? Or using contractors (M52)?

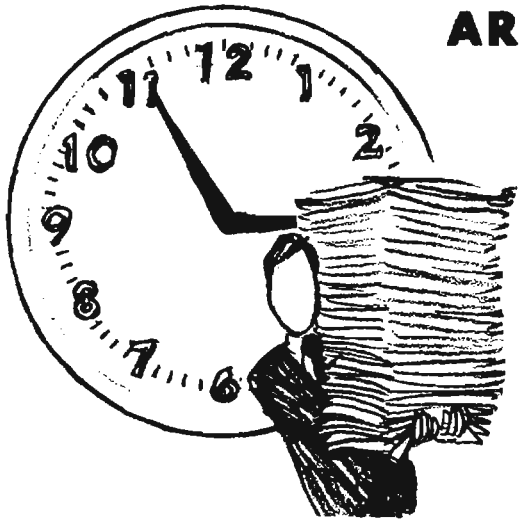
I think the implications of a time-phased action plan in the points brought out above speak for themselves. For the first time we have a uniform rational system for exploring, on a timely basis, the implications of any given move.

We in M have for years suffered in varying degrees of silence about not being notified regarding operational activities until they were at a point where only costly super-priority action on our part could provide the necessary support to successfully complete the operation. Now, under the PMD system, we are participating at the earliest stage in each project. Increasingly we are involved in detailed planning of events beyond the immediate future. This is, and should be, a challenge. We will undoubtedly find that it is easier to talk about planning than to do it. I think, however, we will find that it is more stimulating to take part in the planning than it was to sit around and complain about the lack of it.

NSA has historically been an action-oriented organization. We have all prospered individually and as an organization under this system, but times are changing, and we need to change--like it or not. The PMD system appears to meet that need. Who knows, we might just throw in a little MBO!

The Collectors Corner

A PARTISAN PEEK AT HISTORY



ARE WE WASTING LINGUISTIC TIME?

MARY ROBERTA IRWIN, G52

The EXPERT Sheet referred to in this article is used only in G, but a similar purpose will be served in A by the new Product Source Record and in the field by the Source Contribution Record. B Group is considering a version of its own.

There have recently been a number of articles in the *Technical Journal*, CRYPTOLOG and other Agency publications on language and language processing, but none of these has touched upon the problem of conserving the short supply of linguists for purely linguistic work. This problem can easily be overlooked or minimized by everyone but the linguist involved with current production on a daily basis. Writing as a linguist with thirty years of experience, spent almost entirely in processing [redacted] I want to present this problem as I have seen it and to suggest some possible solutions.

What non-linguistic work is required of the translator?

1. Logging and filing. This is, of course, among the "other duties as required," supposedly performed only infrequently by linguists when an area is temporarily short of clerical help. I would estimate conservatively that this situation has existed, off and on, for at least half of my thirty years. Let me make it clear that I am not criticizing lower and middle management. Managers at these levels have always been acutely aware of the problem; they simply cannot get sufficient clerical help. But translators cannot operate unless and until messages have been properly recorded and filed, so that references can be found; consequently this work devolves upon qualified linguists, often the younger ones, whose linguistic development under the guidance of older and more experienced linguists is thus slowed down.

2. Stamping the security classification at the top and bottom of each sheet of translation paper. Either stamping or writing this classification on in pencil requires a surprising amount of time. The sheets could surely be preprinted. They have been in the past, and no convincing reason for the change has ever been offered the linguist.

3. Providing data for retrieval of information, "valuable for you and necessary to the Agency," which takes "only a few minutes" for each translation. This has taken various forms over the last thirty years, but with the development of computers the trend has been steadily toward adding "just a few minutes more." In 1945 the translator attached to each finished translation a 3 x 5 card giving lane, message number, system and worksheet number. This was soon returned with the serial number, assigned by some now-forgotten ancestor of NSOC, which a clerical assistant entered in the section's permanent records. Today, thanks to the all-powerful computer, which can save untold numbers of man-hours, we in G have arrived at the EXPERT Sheet, simplified to the extent that the translator-analyst has to fill in only 19, or in some cases 20, of the 42 blocks provided, plus the security classification, which must be handprinted at top and bottom. (See Appendix.)

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

Of all this information, only the title, intercept data, system, and worksheet number really have to be provided by the translator. The security classification could certainly be preprinted and each section provided with those classifications it needed. Precedence could be assigned by an Ø5 analyst, who in any case often changes that assigned by the translator. Other blocks, except for two (discussed in the next paragraph), could be filled in by a competent clerical worker, hired for considerably less than the salary of any professional linguist. This presupposes enough clerical help to allow the designated person to complete the EXPERT Sheet as soon as the translation is received and to carry it immediately to the Ø5--another "only a few minutes" task which frequently devolves upon the linguist. It is not permissible to wait until several translations are ready and deliver them simultaneously, for work must not be piled on the Flex Room late in the day. Typists' time is precious.

The two blocks which could not be left to a clerk are numbers 13, now reserved for TAG's (Topic and Area Guides), and 37: KIQ's (Key Intelligence Questions--to be filled in only on

the last three carbons!). Before the addition of the KIQ's and TAG's, the sheet required approximately five minutes. Now those two items require more time than all the rest of the EXPERT Sheet, since a great deal of consideration is needed for each message. What is to be done about these?

Admittedly, translators must be intelligence analysts, for they have to decide what is significant enough to be translated, and in what order of priority, and in addition they must apply their judgment as analysts to the correction and translation of corrupt or telegraphic text. But the assignment of KIQ's and TAG's is a task of intelligence analysis which does not require linguistic ability. Qualified SRA's may be as hard to find as qualified linguists; but since in any case they must review the KIQ's and TAG's assigned by the linguist and since--and this is far more important-- these codings

In conclusion, then, it seems that we are:

1. Stunting the development of our younger linguists by using them as clerical help, thus making it impossible for them to acquire on-the-job training under the guidance of their more experienced colleagues--something which they all need, however excellent their college records may have been and whatever they may have learned in NSA training classes. As the older linguists retire in ever-increasing numbers, this problem is assuming the proportions of an emergency.

2. Taking all linguists, both young and old, out of the linguistic field and into aspects of the job that could be better done by intelligence analysts who do not require linguistic ability. In my own work as a translator-checker, I estimate that I spend about four hours per week on non-linguistic functions. Some translators spend more, a few less. The amount of time seems small, but it represents 10 percent of my working hours per week. If this figure is anywhere near average, can the Agency afford to devote one of every ten of its linguists engaged in current production to non-linguistic operations?

Appendix

~~(TOP SECRET UMBRA)~~

The Cryptolinguistic Association will hold its 10th annual banquet and awards presentation on Thursday, May 29, at the Trojan Horse Restaurant in Silver Spring. The speaker will be our own Jack Gurin, whose talk is entitled, "What's a Nice Guy Like Me Doing in a Job Like This?"

The winners of the CLA Essay Contest will be announced, and also the recipient of the Jaffe Award, which is given each year to someone who has made an outstanding contribution in the language field.

The gala evening will begin with a cash bar at 6:30, followed by a roast beef dinner at 7:30, then the program at 8:30, and at 9:45 a social period which will include dancing. All this for the modest cost of $7.50 to members and $8.00 to guests.

For reservations contact [redacted] on P.L. 86-36 5471(s).

(UNCLASSIFIED)

ANSWER TO

OPTOGRGLY SPEAKING

A reader has chided us for not explaining the "usual rules of the game." According to the Washington Star, these are: (1) Words must be of four or more letters. (2) Words which acquire four letters by the addition of "s", such as "bat," "cats," are not used. (3) Only one form of a word is used. (4) Proper names are not used. According to our puzzle expert, "usually an abridged dictionary is specified beforehand." O.K.:

The following words are to be found in Webster's Seventh New Collegiate Dictionary:

Clog, cloot, clop, clot, cloy, color, colt, cool, coop, co-op, co-opt, coot, copy, crop, crypt, crypto, glory, gory, grot, gyro, loco, logy, loop, loot, lory, orgy, orlop, plot, ploy, poco, pogo, pogy, polo, poly, polycot, pool, poor, porgy, port, portly, prog, root, ropy, roto, tool, tory, troop, troy, typo, tyro.

(UNCLASSIFIED)

ANSWERS TO CLASSIFICATION PROBLEMS

INTERNATIONAL AFFAIRS INSTITUTE

Members of the International Affairs Institute recently elected the following new officers:

President-Elect Robert E. Drake
Members-at-Large [redacted]
Barbara W. Clark
[redacted]
Robert J. McDermott

Also, at the March meeting of the Board of Directors, a new secretary, Robert J. McDermott, was elected to complete [redacted] time in office.

The President, [redacted] and the members of the Board are currently working on a series of projects aimed at expanding the activities of the I.A.I. to more directly involve and benefit all the members of the Institute. The members will also be encouraged to express their ideas and views in a questionnaire which will be distributed in the near future.

P.L. 86-36

(UNCLASSIFIED)

[redacted]

I hope this exercise clearly demonstrates the problems and difficulties involved in determining classifications, and specifically what information needs Codeword or "COMINT Channels" protection. There are eight Classification Advisory Officers at NSA. They are willing to offer assistance in your classification problems, but the responsibility for proper classification belongs to each of us. My advice then is to use the Classification Manual and USSID 3, consult your Classification Advisory Officer when necessary, and most important, take the time to determine the appropriate classification and thus to insure that the proper protection is being afforded.

~~(TOP SECRET UMBRA)~~

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

LETTERS TO THE EDITOR

P.L. 86-36

To the Editor, CRYPTOLOG:

I hope you can find room in your next issue for clarification of the editorial introductory note for [redacted] recent piece on "The Uses of ELINT" (April 1975).

Having established that in the beginning there was COMINT, your note then refers to ELINT as "the other half of SIGINT." Unless P1 has developed a new-new-math which permits more than two halves in a whole, you have (unintentionally, I trust) eliminated the "other third" of our SIGINT family: TELINT.

Confusion on the place of TELINT (Telemetry SIGINT) is as understandable as it is widespread. For years, NSAers thought of it (if at all) as a sub-set of ELINT, largely because it used no COMINT coverwords and because in 1960 USIB had decided to classify it and handle it "like ELINT." A former Chief of P1 was a leader in opposing this "ELINT-by-association" theme; since telemetry's job is to communicate information, it cannot be a "non-communications transmission" in terms of the accepted definition of ELINT. [redacted]

On the assumption that CRYPTOLOG is happy to support its sister publications, I modestly (?) recommend to your readers a two-part SPECTRUM article giving the background of NSA's involvement in telemetry (Vol.1 No.3 and Vol.2 No.1, "Talomatry and How It Grew").

The term "telemetry" is often used with a broad meaning which includes some (but definitely not all) other kinds of "Foreign Instrumentation Signals" (FIS), a term which is appearing more frequently in USIB community papers. (In fact, there is talk that a new NSCID may divide SIGINT into COMINT, ELINT, and FIS.

Telemetry has come a long way in the 20 odd years [redacted] timely [redacted] intelligence support to U.S. Navy and other tactical commanders!

[redacted] V3 P.L. 86-36

The Editor regretfully acknowledges the error and promises it shall not happen again.

To the Editor, CRYPTOLOG:

[redacted] letter in the April 1975 CRYPTOLOG concerning the professionalization problems of bookbreakers, and the related questions posed by [redacted] the Cryptanalysis Editor, in her note, tend to confirm a suspicion that has been growing in my mind for the last five years: the venerable term "bookbreaking" and the importance of the SIGINT produced by its practitioners seem to have become lost in the bureaucratic red tape somewhere in the fog-shrouded ivory towers of operational and personnel management.

This loss of understanding by management goes far beyond the mere fading of a useful term; application of the specialized skill itself has become clouded in management's mind to the point where (in B Group, at least) it is now closely equated with cryptanalysis. [redacted]

[redacted]

The current CA Task Inventory revalidating the COSC job codes provides an excellent opportunity to review and perhaps redefine the term "bookbreaker" and what he does, or should be capable of doing, in terms of job skills. And this letter is my opportunity to offer some personal views towards that objective, based on 31 years of experience in almost every aspect of the SIGINT business, [redacted]

[redacted]

[redacted]

[redacted] And without the bookbreaker's alchemy there is damned little substance (other than TA) from which the SRA can construct a story and garner the kudos that so often rightfully belong to the bookbreaker industriously working in the background to perfect the code so that even more and better secrets can be revealed. The bookbreaker is the individual who created something from nothing!

[redacted]

P.L. 86-36

To the Editor, CRYPTOLOG:

There is need to recognize bookbreaking as a distinct form of analysis, by the establishment either of a separate career field or of an option within a separate cryptolinguistic career field. The cryptolinguistic option of the present language PQE does not test directly for knowledge of analytic principles, use of machine support, of predecessors as models, of statistics, of working aids, etc., all of which are necessary for bookbreaking. And now more than ever these techniques are indispensable for bringing a code to readability, for we are faced with lower volumes and at the same time more difficult codes, as they have been improved through the years.

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

[redacted]

[redacted]

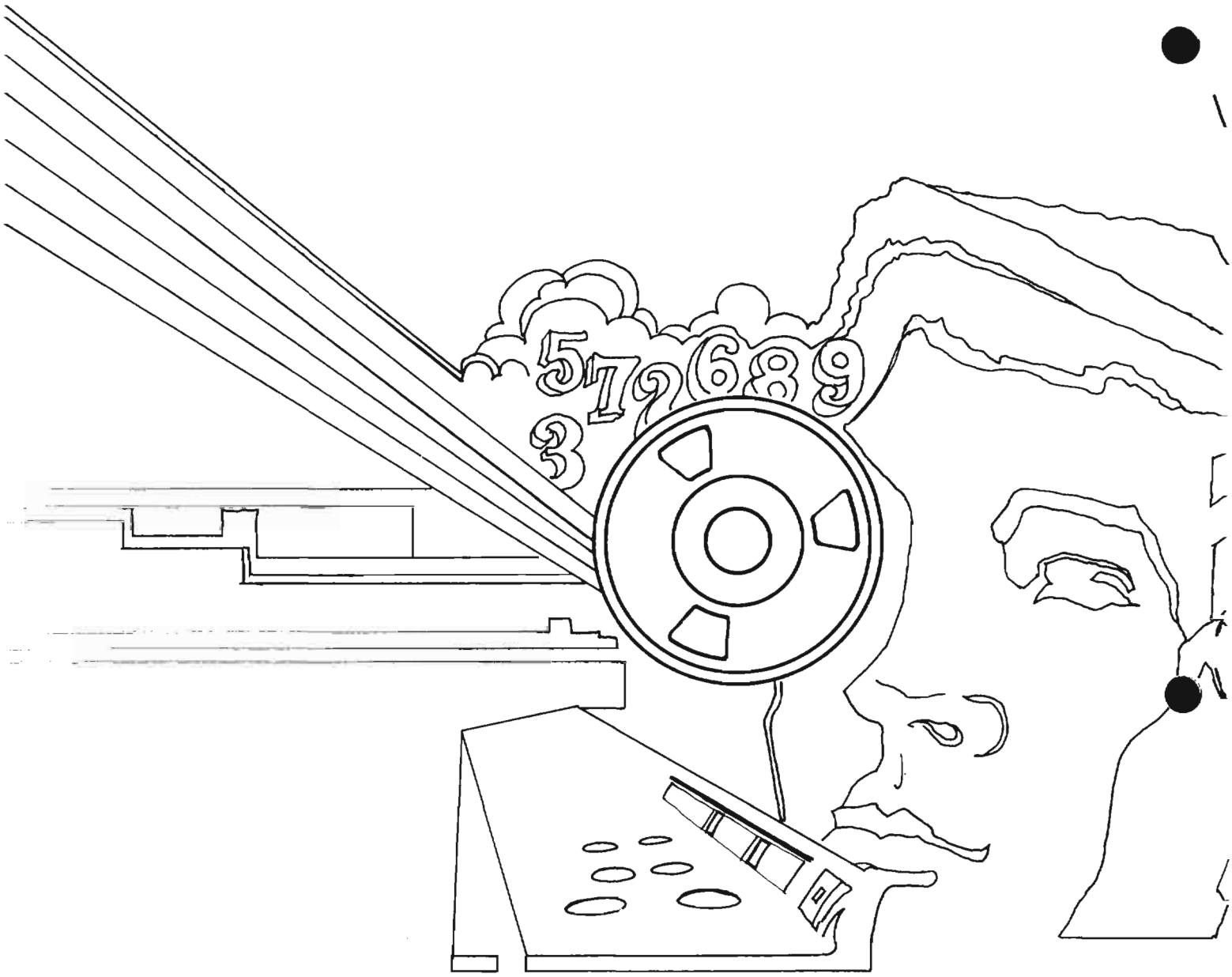
In summing up, my view of the bookbreaker is that he or she is first of all a linguist, but one who has progressed beyond routine translation. It is a highly personal and individual capability. Through some quirk of nature or personality he or she is usually intensely interested in solving the mystery of the unknown: creating knowledge out of meaningless code groups. It is this spark of genius that is the bookbreaker's true value.

[redacted]

[redacted]

~~(CONFIDENTIAL/HVCCO)~~

P.L. 86-36


5 7 2 6 8 9
3