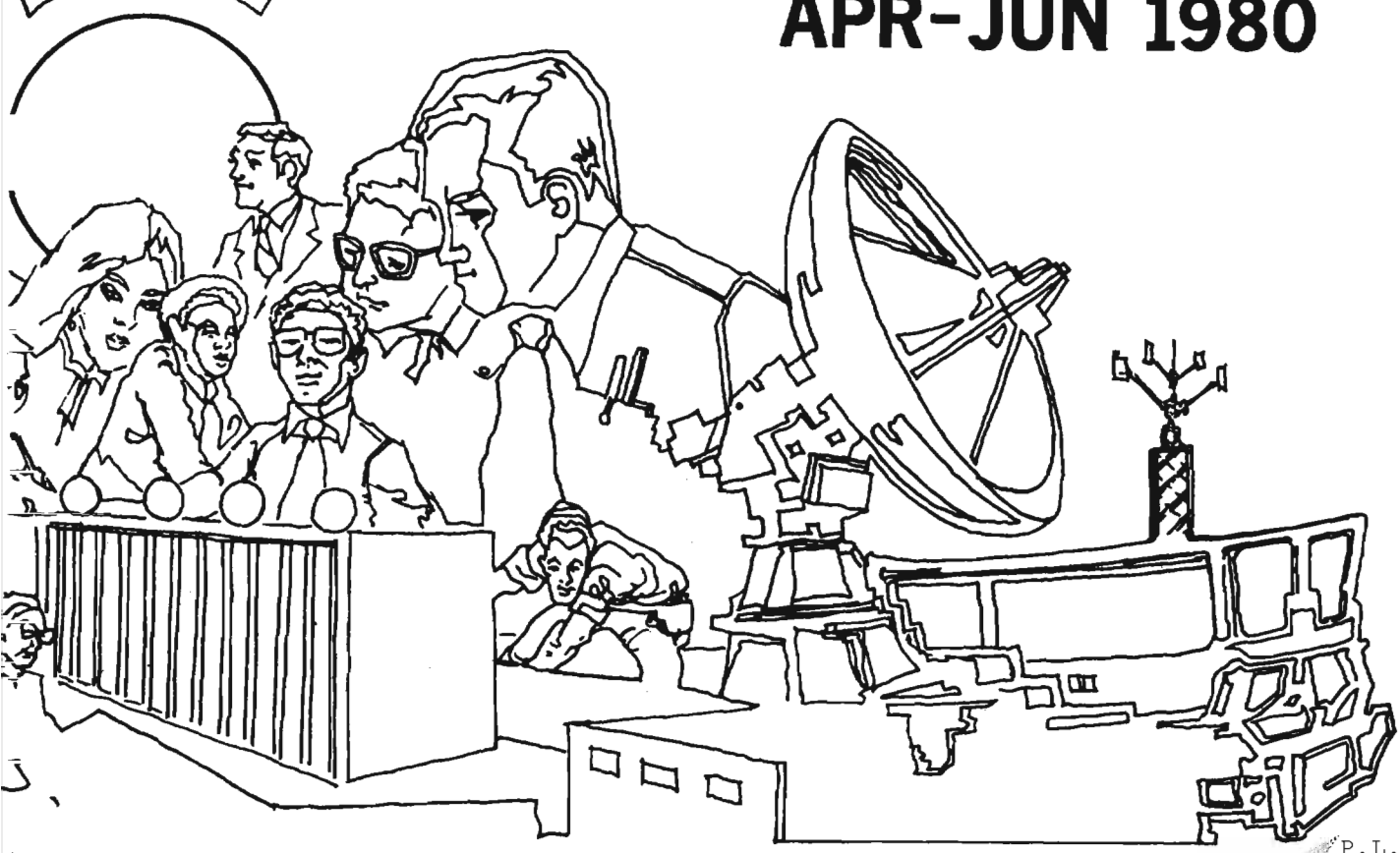
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

APR-JUN 1980



P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 1 JUN 2010~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. VII, No. 4 - 6 APRIL - JUNE 1980

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

CECIL J. PHILLIPS, T4

An address given earlier this year by Mr. Phillips before the Computer and Information Science Institute

DATA FLOW — Challenge of the 1980s (U)

When I was asked if I would give a talk at CISI and I agreed, I knew what I wanted to talk about, but I was not sure what kind of title I wanted to give it. I settled on the Data Flow title, although a more proper title might have been "Data Flow, Feedback, Control and Inter-Process Dynamics"—all of which are involved in what I consider to be our main EDP challenge for the 1980s.

(U) Perhaps I should also state at the outset that the challenge is to everyone in the SIGINT process, not just people in the EDP field. As we keep saying in our budget justification, computers are integral to virtually every step in the SIGINT process, either by performing a function, by delivering the data to a human to perform a function, or by taking the results to the next process.

(U) Let me talk for a minute about data flow's role in the whole picture, which, as far as I'm concerned, is central to the whole process. Without data flow there is no need for feedback and control and there is nothing one could call inter-process dynamics.

(U) I think people have always understood that knowledge of data flow is useful to understanding processes whether they be human or machine. When I first made contact with Automatic Data Processing about 35 years ago, one of the basic elements of planning ADP jobs was to produce a flow chart. Flow charts usually showed the movement of material, which in our business has always been data—whatever its form. In those days flow charts (with which I never felt totally at home) usually showed functions such as edit, punch, sort, list, make corrections, etc.

(U) These functions were either manual, as in the case of "edit," or manually initiated as in the case of "sort," "list" and others. The key thing about this is that virtually all the inter-function actions were by humans responding to written or verbal instructions. These human interfaces represented both good news and bad news. The good news was that function-to-function interface was easy to take care of, but the bad news was that it worked only as well as the humans understood and cared about what they were doing.

(U) With the introduction of the stored program computer, flow charts to show data and control flow became basic tools for planning how to write computer programs, usually showing functions at a much more detailed level than the case I described before. Stored programs permitted data to be passed from one process to another without human interface, but the size of computers and the complexity of programming meant that the data went external to the system time and time again. Thus, the human interfaces I mentioned were still very much in evidence. However, there was automatic feedback within programs. After all, one of the main attributes of a computer was its ability to modify the stored program, or modify the data, but almost any inter-program feedback was handled by humans.

(U) Today, there are still hundreds of processes in which inter-process communication is via human beings. That would not be so bad if I were talking about humans linking processes through interaction at a CRT. But I am not! I mean that there are still hundreds of processes where the result goes external to something like a print and any result going to a next process gets entered by hand. Sometimes this is via punched cards, and there are still a few examples using paper tape to re-enter data.

(U) Another of the problems in the way we treat data flow today lies in the fact that too many processes are still batch processes. These are probably satisfactory for treating single-direction flows of data, but are not very compatible with feedback and control—especially if we expect feedback and control to have any effect while actions are still taking place. I believe there are much better ways of treating data than these current batch flows and these new methods are also part of the challenge for the 1980s. I will get back to this later.

(U) All of this reference to past and present data flow and flow charting brings me around to what I consider the challenge of the 80s—namely, how to make a substantial leap forward in the way the flow of data is understood and treated and to use this knowledge to improve the whole SIGINT process.

(U) Why is there a challenge?

(U) I believe there is a new kind of challenge here because I believe that for the first time all the capabilities necessary to cause data to flow from collection to customer, with appropriate feedback of control information, are present. At the same time, there are capabilities which will enable analysts—separated by space—to work together as though they were sitting side-by-side. I realize that over the years there have been a number of major technological developments, each of which seems to be a breakthrough, but I believe that the 1980s can see us put it all together well for the first time so as to make a breakthrough in the only area which will have a long-lasting and far-reaching effect—namely, to begin to process and handle *information*, rather than data, throughout the SIGINT system.

~~(C-CCO)~~ Just for a moment, let's take a look at the key ingredients.

► Terminals/access devices. In the 1980s, for the first time we will have enough terminals so that virtually everyone in the SIGINT system will have some kind of access to one. By the end of the decade we ought to have a terminal or access device on every desk. The only weak spot may be in the area of full graphics, an area whose application to SIGINT is still to be developed (except for some highly specialized cases).

► Concentrators/Terminal Sub-Systems. We have these in great profusion. It is not that these perform a unique function; they are just convenient boxes between terminals and mainframes or networks, occasionally providing extra computer power or extra storage.

► Networks and Communications. These, along with the terminals, are the real breakthrough. For the first time we are beginning to have what is needed—communications to support interactive processes at any distance we want. [redacted] -and by the end of 1981 to most major points in the SIGINT systems, wherever they are.

► Main Computers. As you well know, there are plenty of these of almost every type.

(U) In short, we are soon to have the technical capability for every user/analyst at every terminal to talk to every other analyst and every other process via his keyboard.

(U) If all of this is true, what is the challenge?

(U) The challenge is to make it all do some useful work in the production of SIGINT. The challenge is to interface people with information, not just terminals with computers. This is where the payoff, the success and the rewards are. Since there are a lot of computers already doing many of these things, what makes the 1980s special?

(U) I believe there are at least three main areas of challenge in the 1980s.

► Causing the data to flow smoothly from collection to output reports.

► Treating the data in natural information units which foster the development of better analytic approaches and feedback and control.

► Developing techniques for *teleanalysis*, a term which I have cointed to describe methods by which two analysts may collaborate over a distance.

(U) Let's take a look at the flow problem first.

~~(C-CCO)~~ Causing SIGINT data to flow effectively and smoothly from collection to user output in natural information units with appropriate feedback and controls sounds like a goal that has been around for a long time, but I think that for the first time we can realize the full value of machine interaction and feedback which actually influence processes while they are still going on. At a kind of top level design, this probably sounds pretty straightforward. At that level it is. However, at the detail level, it means thousands of processes which have to be understood in terms of all the other processes to which they relate. These other processes may be adjacent, but things which affect them may be several levels away. [redacted] This means that there are so many interrelated effects that understanding them all is out of the question. And this is precisely where the greatest challenge comes—that is, finding a method for describing the interfaces and then exploiting it to connect them.

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

(U) I think it important to understand that what I am suggesting is not simple—because I am not just talking about standardization at low levels of protocol and format. Many of these are already covered in PLATFORM and some of the format conventions are covered in USSIDs. What I am really talking about is a set of information level protocols—things

which humans do now, in the best cases almost without thinking.

(U) Such an example might be where an analyst knows instantly where a mis-identified message must go to get it back on track. At the same time, most of our current processes simply dump data back into the system. The challenge, of course, is to develop automatic re-routing schemes or man-machine interactive processes which allow for re-entry and re-routing in such cases.

(U) I think this dictates the need for developing a convention for annotating and labeling the error transactions so they can be re-entered into the process to produce a new result which is a combination of the computer process and the man-machine interaction process. If the person annotating the transaction knows exactly where the erroneous data goes, the problem is relatively simple. If he simply knows that it is wrong and wants to send it back, the problem is much more complex. This is especially true of the problem of how to label it in order to get a different result the second time through the system.

(U) This might be fairly straightforward if all feedback is from a single class of process back to the collector. In real life this is not usually the case; rather, the feedback comes from all parts of the system. Thus, there is the need to be able to accommodate different levels and kinds of information.

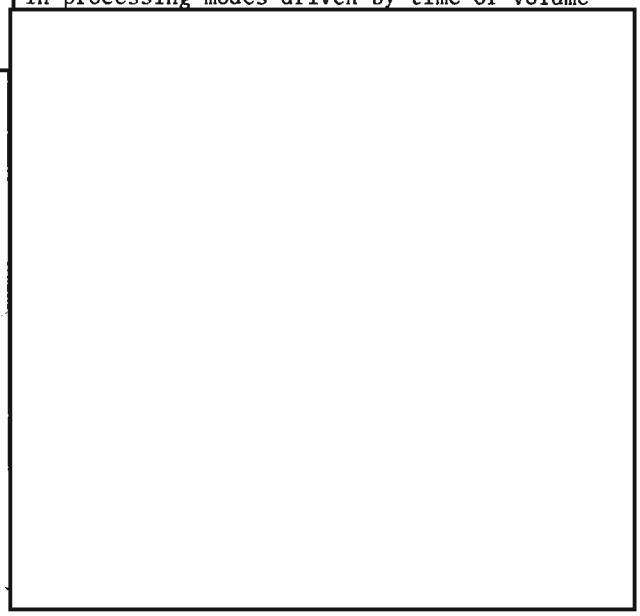
(U) Up to now, we have been doing all of the things I am discussing—particularly feedback—by human action, mostly on a hit-or-miss basis. There have been some near real time collection control groups, but their effectiveness has been limited by slow and erratic feedback to them from analysis, by slow and erratic methods for delivery of information back to the collectors, and often by slow and erratic reporting and communications with the collectors.

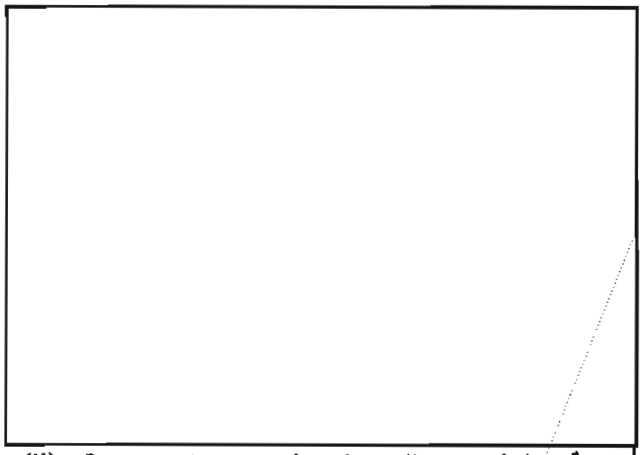
~~(C-CCO)~~ Let me make it clear that these groups have done a super job, often with very limited help from the computer types. So there is part of the challenge—to help refine the existing processes and extend control processes to all parts of the system to manage processing, analysis and reporting, as well as collection. It has been said that there are more signals in the air than we can collect, more signals collected than we can process, and more signals processed than we can transcribe or decrypt and then report on. The net effect is that we must be able to select and filter the flow at all points in that flow.

(U) Much of what I have said is fairly simple on a case-by-case basis. As I noted earlier, the complication comes in looking at the whole picture or a large fraction of it. There are also a few other complications in that broad interprocess communication is not the goal of everyone. Systems designers are likely to have a goal of optimization within their own domain which is usually sub-optimization as far as the overall SIGINT process is concerned. Further, every manufacturer and creator of new software packages is out there being as creative as possible to give his system some unique features. Users of the overall system are likely to have to keep running just to stay even with all the variations.

(U) The second part of the challenge had to do with treating data in more natural or "event-driven" units so that feedback and control have more meaning. An alternate way of thinking of this is to consider dealing with units of data.

~~(C-CCO)~~ Perhaps this is naturally inherent in a good system, but we have been so long in processing modes driven by time or volume





(U) Because transactional or "event-driven" processing has strong implications of more timely operations, it may seem that I am really discussing time-sensitive processing. Transactional processing does make these things possible but it does not demand it. You can save work queues in transactional systems as well as in batch, and in a transactional system you ought to be able to save them even more intelligently.

(U) A third and final part of the challenge of the 1980s, as I see it, is to develop techniques for *teleanalysis* or *telesynergism*—terms I made up hurriedly to describe joint analysis done by two or more people over distance. Let me explain what I believe should be possible here. I am talking about a form of teleconferencing in which man-machine interaction takes place with two or more people at separate terminals operating against the same data, where the data may be a message, entries in the data base or any other form.

(U) There is probably some tendency to equate this to teleconferencing, but it is a level above teleconferencing. It is teleconferencing in which the analytic problem is at least part of the medium.

(U) We are optimistic that the seeds of such ideas can begin to develop as soon as network connections are established with collaborating analytic centers. The goal is to see the multiple work forces at various centers integrated through this telesynergistic bond so we can use the work force better or tackle more complex problems.

(U) I have no doubt but what it will take a long time to really accomplish this on a broad scale. First, we have to hit people with two-by-fours to get them to treat problems interactively on computers where one person and one terminal is involved. But in time the software and the technology will improve and the problems to be solved will become bigger or harder, or both, so there will be an incentive to develop telesynergism.

(U) At the same time, programmers and systems developers also need to be touched by the two-by-four to remind them that their job must be to simplify the interface to the system so it can be more readily used. The challenge to all of you is to help develop the system tools and to help explore the ideas with the analysts who are bold enough to consider them.

(U) I think it was Mark Twain who said that there is no death like being talked to death, so let me conclude with a brief summation.

(U) My key point about the challenge is that EDP people and communications people must understand the whole system, that is, all the parts, and all the processes and how they interact with each other—whether man or machine. Another name for this is total data flow—from start to finish—including feedback.

(U) Given some understanding of the system —the depth of understanding will naturally vary with one's role—I see the challenge as one of developing full information interfaces between the parts of the system, not just signal and processor interfaces. To me, this implies overall design and and overall approach—real, top-down design from the *very* top, not from some local peak.

(U) In a larger sense, it is the challenge to everyone in SIGINT to make the data flow from process to process and to make the feedback data and contraol data flow where they are needed. In short, this means to make every last piece of the SIGINT system fully interoperable with all the rest.

(U) I think that this is a challenge which can pretty well occupy everyone during the 80s.

* * * * * * * * * * * * * * * * *

(UNCLASSIFIED)

SOLUTION TO NSA-CROSTIC No. 30.

From a Letter to the Editor on COPES, by Donald Y. Barrer, P1, CRYPTOLOG, September 1978.

"My concern stems from admissions made privately and off the record that when COPES objectives satisfaction is low we [alter] the objectives so that the rate of satisfaction looks better, and when things look too good we add objectives to preclude a cut in resources. This should not be surprising; it is a natural response."

(UNCLASSIFIED)

* * * * * * * * * * * * *

A TRAFFIC ANALYST LOOKS AT COMPUTERS

[redacted] P14 P.L. 86-36

In the world of computers, I am an amateur. I have used them as tools in various analytic jobs for many years, but always with someone else acting as intermediary, either a programmer or a systems analyst. I went through most of the same frustrations and associated withdrawal symptoms that other analytic people did when our "traffic" was taken out of our hands and file cabinets and put into the bowels of the basement somewhere out of sight and out of reach except through the offices of these intermediaries.

I frankly think that, contrary to popular opinion, we analysts were not all afraid of computers. Maybe some were, but not all. But what we all did share was the realization that our processing cycle was no longer solely under our control. Our data was in a loop that went through someone else's area of control: while it was in the computer, we had no control over it. Someone had control, of course, but that someone was never us. The people running the system did not work for the analytic people. This is not to say that they did a bad job or that they did not try to support us in the best way they knew. But prior to computers, when traffic came into my shop, it was "my traffic" and I kept it under my control for as long as I had need of it. The people who handled it for me worked for me (and were rated by me). If that sounds proprietary, it is because it was a proprietary kind of system. Today, however, there is very little of the proprietary feeling among analytic people. It isn't really "my traffic" any more.

All this is not meant as a harangue about computers, but is put forward to show where I'm coming from, so you can put the remainder of these remarks in context.

While I have not yet relinquished my sheltered role with respect to computers, I have been spending some time at the keyboards of several CRT terminals. For the most part, I have been trying to do (or simulate) an analytic task, usually some aspect of traffic analysis. Since any traffic analyst these days must work within the framework of computers (all of his data is inside them somewhere), I was motivated to see just what "doing TA on a terminal" really amounted to. This represents a first report of that venture, with all of the biases that first reports commonly have. I am not finished looking, but I thought I would put down three early impressions based on my own hours at the keyboards.

► As I look over my early notes to myself, I am impressed about how often I had typed in a TAPQE problem involving several days traffic, all in upper case (just like an old-fashioned Morse problem for those of you who remember), and since all the commands I was using were in lower case, I kept finding bits of lower case data in the traffic. Later, as I became more familiar with the problem (I think I could have recited each page of the traffic by the time I was through), I began to notice that pieces and lines were missing. I really don't know why the erasures and writeovers happened in each instance, but often I noticed that the cursor on the screen ran a bit behind me when I was entering data; I might stop and glance at the cursor position and not realize that the cursor was running behind. There may well have been other basic reasons for the losses and accidental writeovers, but the experience left me very wary about typing data in at anything near my normal typing speed—which is not terribly high. I also spent some time trying to think out defensive strategies for avoiding the loss of data, such as always working on a copy of a file rather than the file itself, making a habit of storing off the working file fairly often, as frequently as every few lines on material I was anxious to protect. The problem needs more attention, both by computer people and by system designers, since we already lose too much data around here by more classical methods, and really don't need new and inventive ways to lose still more; I don't have any solutions to offer, only a warning that the ease with which data can be altered or erased is scary and will not go away just because we don't want to talk about it. At least part of the problem lies in perceiving that it has happened at all; most of my errors were not noticed until

some later time.

► The next problem I had is a personal one. I wear glasses—bifocals. In order to read the screen I have to bend my head back so that I can see through the bottom part of the lens, where its reading prescription is. A whole day of that is a little more than I want to think about. When my neck gets sore, I have to stop. My choice, I suppose, is to buy another set of glasses, just for reading CRT screens. Or maybe the government will buy them...

► I have heard people say that when we get CRTs on everybody's desk, we can go to a paperless system. Don't you believe it. Have you ever seen a computer printout? Those folks use up more paper than we ever did, with yards of stuff preceding the actual print. Nevertheless, the point I want to make is that I found the screen too small to do anything like a diagram or a tabular lising of continuities. Having experimented with both the PQE problem, which was a simple continuity problem (similar to the final problem in TA-100), and with several CRYPTOLOG problems, I found that I could not keep track of recoveries in any orderly way when all I had to work with was the screen, even one like MYCROFT/CARONA which can be moved around and divided into parts. But all that changed when I decided to try to work with a combination of printout and screen. I used the printout as a basic worksheet, making notations on it from time to time, then adding them to the screen and generating another printout. This will work if the printer is fairly close (I don't consider the basement close to the second floor), and not so busy that one has to wait more than a few minutes for the output.

* * * * * * * *

Because of my interest in "doing" problems on or through the computer, I have been interested in encouraging others to try it also. If you have access to a terminal and would like to try it, let me know. Send me a note (to wes at carona, if you can access PLATFORM), or call me on 3360s.

As analytic people gain more experience in this area, we should find ways to plow that experience back into better support and better systems. With this in mind, we in P14 have set up a file called "whydontwe" where we record various bits and pieces of reactions to the terminal, system, network, or whatever. Not all of it is literate, and some of it looks sort of dumb when re-read at some later date. But it is what we thought or felt at the time, and some of my earlier items formed the basis for some of the above. I would encourage you to do the same. If you want to see what dumb things we said, why don't you have a look (if you're a CARONA user) at the file /u3/pin/why/whydontwe. If you have an idea but don't know who to give it to, send it to me. If there's enough interest in this sort of thing, maybe the editor would be agreeable to a regular feature (assuming, of course, that they're printable).

From the Editor: CRYPTOLOG will be happy to publish any printable responses to Wayne's solicitation (and to chuckle privately over any which are not.)

P16 Language and Cryptologic Library

[redacted] T12, Librarian of the P16 Language and Cryptologic Library, wishes to advise readers of the excellent collection of older works on cryptology available there, some of which date back several centuries. Unfortunately, items in this collection are not available to be taken out, but must be read on the library premises, which are at FANX, Room B3526. For further information, [redacted] may be called on 8873s. P.L. 86-36

A partial listing of volumes in this collection is given below.

Bazeries, Etienne. *Les Chiffres Secrets Devoiles.* Paris: Librarie Charpentier et Fasquelle. 1901.

Booth, Williams Stone. *Some Acrostic Signatures of Francis Bacon.* Boston: Houghton Mifflin Company. 1909.

Breithaupt, Christian. *The Art of Deciphering of the Science of Solving and Reading Secret Writings. Together With a Historical Account of Various Methods of Secret Writing in Use Amongst the Ancients and in More Recent Times.* Helmstedt (Germany). 1737.

Breithaupt, Christian. *A Historical, Critical, and Detailed Disquisition Concerning the Various Types of Secret Writing Employed by the Ancients as well as by Those of More Recent Vintage, Together with an Account of the Art of Deciphering.* Printed at Helmstedt (Germany). 1727.

(UNCLASSIFIED)

Cardan, Jerome Girolamo. *21 Books of Jerome Cardan, a Doctor of Milan, on Subtilitas.* Printed at Basle. 1554.

Champollion, Jean. *Grammaire Egyptienne.* Paris: Typographie de Firmin Didot Frères. 1836.

Donnelly, Ignatius. *The Great Cryptogram: Francis Bacon's Cipher in the SoCalled Shakespeare Plays.* Chicago: R. S. Peale and Co. 1888.

Dröscher, Ernst. *Die Methoden der Geheimschriften.* Leipzig: K. F. Koehler. 1921.

Figl, Andreas. *Systeme des Chiffrierens.* Graz: Verlag von Ulr. Mosers Buchhandlung. 1926.

Fiske, Gertrude Horsford. *Studies in the Bi-Literal Cipher of Francis Bacon.* Boston: John W. Luce and Son. 1913.

Frederici, Johannes Balthasar. *Cryptographia or the Art of Secret Writing.* Hamburg. 1684.

Gallup, Elizabeth Wells. *The Bi-Literal Cypher of Sir Francis Bacon.* Third edition. Detroit: Howard Publishing Company. 1901.

Greely, A. W. *War Department Telegraph Code.* Washington: Government Printing Office. 1906.

Gross, Hans. *Handbuch für Untersuchungsrichter als System der Kriminalistik.* Part II, sixth revised edition. Munich, Berlin and Leipzig: J. Schweitzer Verlag (Arthur Sellier). 1914.

Harvey, Henry. *Harvey's Vanguard Code.* New York: Code Press of Henry Harvey. 1892.

Jacobus de Silvestris of Florence. *Rules of Secret Writing.* Rome. 1526.

Klüber, Johann Ludwig. *Cryptographik, a Manual of the Art of Secret Writing.* Tubingen. 1895.

Lacroix, Paul. *La Cryptographie.* Paris: Adolphe Delahays Libraire-Éditeur. 1858.

Lange, André and Soudart, E. A. *Traité de Cryptographie.* Paris: Libraire Félix Alcan. 1925.

Locard, Edmond. *Traité de Criminalistique.* 2 volumes. Lyon: Joannes Desvigne et Cie. 1935.

Loria, Gino. *Le Scienze Esatte Dell'Antica Grecia.* Modena: Antica Tipografia Soliani. 1893.

Meng, John J. *Despatches and Instructions of Conrad Alexandre Gerard, 1778-1780.* Baltimore: The Johns Hopkins Press. 1939.

Meyer, H. R. *The Commercial Telegraph Code, to Meet the Requirements of the London Telegraph Congress of 1879.* New York: American Code Co. 1880.

Plum, William R. *The Military Telegraph During the Civil War in the United States.* 2 volumes. Chicago: Jansen, McClurg and Company. 1882.

Porta, Giambattista. *Twenty Books of Natural Science.* Leiden. 1644.

Romanini, Vesin. *La Cryptographie Dévoilée.* Paris: Typographie Hennuver. 1857. Author also listed as Vesin, C.F.

Sandler, Rickard. *Chiffer.* Stockholm: Wahlstrom and Widstrand. 1943.

Scotus, Johan Maria. *Four Books of Secret Writing.* Naples. 1563.

Sympson, S. *A New Book of Cyphers.* London: John Bowles. 1750.

U. S. Bureau of Navigation (Navy Department). *The International Code of Signals for the Use of All Nations.* Washington: Government Printing Office. 1875. Also available in revised edition, 1894.

U. S. Department of State. *The Cipher of the Department of State.* Washington: Government Printing Office. 1876.

Valerio, P. *De La Cryptographie.* Paris: Librairie Militaire De L. Baudoin. 1893.

Velasquez, Manuel M. *Codigo Universal de Correspondencia Secreta.* Mexico. 1926.

(UNCLASSIFIED)

...and in a more modern vein... (U)

(U) [redacted] Chairman of the Bookbreakers' Forum, suggests the following publications as essential reference works for those in the field of cryptolinguistics. If you are interested in obtaining any of these documents, call [redacted] on 1103s. All are classified TSC. P.L. 86-36

Buck, Stuart H., [redacted] (U) *CRYPTOLOG*, July 1977.

~~(TSC)~~ [redacted] EO 1.4.(c) P.L. 86-36

[redacted] *Italian Bookbreaking* ~~(TSC)~~. National Security Agency Technical LIterature Series, Monograph No. 6, 1965. P.L. 86-36

~~(TSC)~~ The original paper was written in 1943 while bookbreaking was still being done on the Italian Military and Air Force codes. Soon after, the Italians surrendered themselves and their codebooks. The bookbreakers then had an opportunity to compare their results with the original of PEGASO, the Italian title for their latest Air Force code. A very interesting account of a specific effort which can also serve as a primer on bookbreaking.

Swift, Katharine L., "Some Problems and Techniques in Bookbreaking" (U). *NSA Technical Journal*, Vol. XI, No. 1, Winter 1966.

(U) A concise view of what codes and bookbreaking are all about, and some interesting war stories. Just the thing to start out on.

Swift, Katharine L., *Standards and Techniques of Code Reconstruction* (U). National Security Agency Technical Literature Series, Monograph No. 5, 1965.

~~(S-CCO)~~ Reprint of a 1955 paper (S51,126). Designed for code problems of the 1950s which were [redacted] codes of classic configuaration. Rich in illustrative anecdotes and strong on first principles. Written when card sorters were obsolete but computers were still in their infancy. A must.

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

Swift, Katharine L. and Oliver, Jean. *Collected Articles on Code Reconstruction* (U). Cryptanalysis Department, National Cryptologic School (S-212,802). Revised Edition, 1976.

P.L. 86-36

~~(C-CCO)~~ A collection of shorter articles on assorted topics of relevance to bookbreaking. It can be thought of as a supplement to *Standards and Techniques*, above, which serves to increase its scope.

From the Editor: You should add to the preceding list the following bookbreakers' "must" which has just been published.

[redacted] *The Structure of Codes, Part I: Classic Codes* (U). P16 Cryptolinguistic Series No. 1, 1980 (S-221,647).

~~(C-CCO)~~ An annotated survey of various codes, both U. S. and foreign, used during the first half of this century. This work also includes a comprehensive bibliography of in-house and open source publications on bookbreaking.

(UNCLASSIFIED)

GEOGRAPHIC TRIVIA

- Each of the United States has a highest and a lowest point. Most everyone knows that the highest high point is in Alaska (Mount McKinley, 20,320 feet), while the lowest low is in California (Death Valley, —282 feet). But do you know which state has the *lowest* high, and which has the *highest* low?

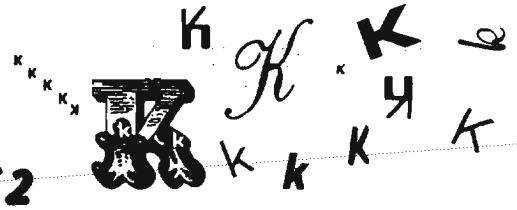
- Many of the largest cities in the U.S. are *not* state capitals. In fact, the state capital with the largest population, according to 1975 Census Bureau estimates, is the *eleventh*-ranking U.S. city. What is it? And what are the place and show capitals? (Old-time trivia players, to whom Boston has always been the most populous capital, will be dismayed to find out that its 1975 population of 636,725, is fourth largest.)

Answers on Page 15

(UNCLASSIFIED)

OH, K!

T152



P.L. 86-36

In a jargon-rich environment like NSA, we are used to the acronyms and abbreviations that enable us to express complicated thoughts in a reasonable amount of space, either physical or temporal. It is inevitable that some abbreviations will have multiple meanings. For the multi-equivalent championship, though, I think we should nominate the steadfast multiplier K. One can envision a question on a future version of the Computer Systems PQE:

Question: K = ?

a. 1000
b. 1024
c. 512
d. 4096
e. DDT

Correct Answer: a, b, c, e, and probably d

a. The classic abbreviation derived from the Greek prefix *kilo-*. Often written in lower case. You can be sure 1000 is meant when the quantity measured is dollars or a standard physical unit, e.g., kHz.

b. A frequent unit of computer memory (whose lengths are almost always powers of two), as in 64K words, meaning 65536. 65K is also used and has the advantage of corresponding to the common use, as in a. above. But the use of K = 1024 is becoming more common because of its precision (64K, K = 1000 is an approximation while 64K, K = 1024 is exact) and the ease of computing the size of memory as it doubles (2*64K = 128K, while 2*65K = 131K).

c. The somewhat self-contradictory "K octal," i.e., 1000_8. A unit often used by those reading displays or dumps.

d. 1000_{16}. I have never actually heard this one used (I don't mix much with users of hexadecimal), but I suspect it's out there. I guess we should be grateful that at least we're not using a number system with a large enough base that K might also be a digit (in which case it would have value 20).

e. See a recent Agency organziational chart.

So, the next time you hear a "K", make sure you get onto the speaker's base!

O.K?

OH, K! (PART II)

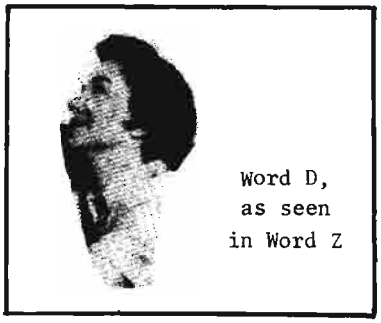
Where did everybody go?

As a result of the recent reorganization which did away with the K organization and sent its people off to various other elements, CRYPTOLOG has been receiving a number of returned subscription copies which had been distributed to K addresses.

So if you used to be in K, and would like to continue to receive CRYPTOLOG, please call (on 1103s) or drop a note (P1, CRYPTOLOG) to let us know your new address.

NSA-Crostic No. 31

by dhw



Word D, as seen in Word Z

A. "_____ and speak each other in passing." "Tales of a Wayside Inn," Longfellow. (6 wds)

84 68 166 255 206 23 179 270 222 103 195 19 273 76 57 148 110 177 123 133 47 263 7

B. Prudent-sounding state capital

30 39 63 174 143 238 279 159 59 9

C. Of maximum fusibility

230 3 244 18 101 207 257 139

D. Hollywood leading lady (1924—), active 1950—1959, in such films as *Crash Landing*, *Donovan's Brain*, etc. (Full name)

240 147 12 186 272 226 252 276 210 32 10 40 168 219 108 64

E. Harmonious-sounding state capital (3 wds)

176 124 201 278 53 271 13 259 145 202 104 100 107 27 241 161 185 169 88

F. Mechanism of a firearm that expels the spent cartridge

211 87 105 109 167 34 146

G. Cereal grain

138 197 203

H. Rigorous; unadorned; grave

60 85 233 116 131 220 162

I. Romantic-sounding town in Florida, seat of Osceola County

96 180 190 72 243 163 130 113 221

J. Full of plots; treacherous

175 80 115 62 196 149 117 208 181

K. Sibling's daughter

141 158 199 89 194

L. Fate, at a turn of the card (4 wds)

5 28 52 120 73 234 128 25 43 144 173 213 231

M. Secessionist province of N Ethiopia

157 275 260 256 251 78 232

N. Women as mates, says Thurber, should be those "who have great constitutional strength and are not _____."

24 65 127 223 160 183 29 36

O. Timid; full of fears

8 277 54 51 97 91 242 135

P. Learned

95 106 155 212 266 69 264

Q. Building for the storage and maintenance of locomotives

132 235 56 214 182 82 140 38 229 248

R. Knotted

178 164 218 215

S. Toast _____ (3 wds)

258 249 90 21 200 269 137 125 151

T. In pointing out why a fifth of Scotch on the bar was preferable to major brain surgery, he explained, "I'd rather have a _____." (9 wds)

86 254 67 93 205 6 102 126 75 4 250 261 50

224 152 265 83 262 70 225 112 119 136 44 79

237 17 191 247 165 31 198 150 134 37 55 98

U. The property of being not separable into parts

268 41 253 58 184 71 142 14 246 216 204 48

20 1

V. The original large-scale-robbery-caper movie (1955)

193 228 35 111 92 114

W. In Germany, units of local government

122 154 121 45 129 26

X. Hairy; rough with bristles

94 11 217 156 239 81 187

Y. Sour

16 77 66 209

Z. The only film in which Word D co-starred opposite her husband (1959) (4 wds)

188 33 192 267 15 22 61 171 2 74 42 99

274 49 245 227 170

Z_1. Capital city of New Caledonia

46 153 236 118 172 189

■	■	1 U	2 Z	3 C	4 T	■	5 L	6 T	7 A	8 O	9 B	10 D	■	11 X	12 D	13 E	14 U	15 Z	16 Y
17 T	18 C	19 A	■	20 U	21 S	22 Z	23 A	■	24 N	25 L	26 W	■	27 E	28 L	29 N	30 B	31 T	32 D	33 Z
■	34 F	35 V	■	36 N	37 T	38 Q	39 B	■	40 D	41 U	42 Z	43 L	44 T	45 W	46 Z_1	47 A	■	48 U	49 Z
50 T	51 O	■	52 L	53 E	54 O	55 T	56 Q	57 A	58 U	59 B	60 H	61 Z	62 J	63 B	64 D	■	65 N	66 Y	67 T
68 A	■	69 P	70 T	71 U	72 I	■	73 L	74 Z	75 T	76 A	77 Y	78 M	■	79 T	80 J	■	81 X	82 Q	83 T
■	84 A	85 H	86 T	87 F	88 E	89 K	90 S	■	91 O	92 V	■	93 T	94 X	95 P	■	96 I	97 O	98 T	99 Z
100 E	■	101 C	102 T	103 A	104 E	105 F	106 P	■	107 E	108 D	109 F	110 A	111 V	112 T	113 I	■	114 V	115 J	■
116 H	117 J	■	118Z_1	119 T	120 L	121 W	■	122 W	123 A	124 E	125 S	126 T	■	127 N	128 L	129 W	■	130 I	131 H
132 Q	133 A	134 T	135 O	■	136 T	137 S	138 G	■	139 C	140 Q	141 K	142 U	143 B	144 L	145 E	146 F	147 D	148 A	149 J
150 T	151 S	■	152 T	153Z_1	154 W	■	155 P	156 X	157 M	■	158 K	159 B	■	160 N	161 E	162 H	■	163 I	164 R
165 T	166 A	167 F	168 D	169 E	170 Z	■	171 Z	172Z_1	173 L	174 B	175 J	176 E	177 A	■	178 R	179 A	180 I	181 J	■
182 Q	183 N	184 U	185 E	186 D	187 X	■	188 Z	189Z_1	190 I	■	191 T	192 Z	193 V	194 K	195 A	196 J	197 G	■	198 T
199 K	200 S	201 E	■	202 E	203 G	204 U	205 T	■	206 A	207 C	208 J	209 Y	210 D	211 F	212 P	■	213 L	214 Q	215 R
■	216 U	■	217 X	218 R	219 D	220 H	221 I	222 A	■	223 N	224 T	■	225 T	226 D	227 Z	228 V	229 Q	230 C	■
231 L	232 M	233 H	■	234 L	235 Q	236Z_1	237 T	238 B	■	239 X	240 D	241 E	242 O	243 I	244 C	245 Z	246 U	247 T	248 Q
■	249 S	250 T	251 M	■	252 D	253 U	254 T	255 A	256 M	257 C	258 S	259 E	■	260 M	261 T	■	262 T	263 A	264 P
■	265 T	266 P	267 Z	268 U	269 S	270 A	271 E	272 D	■	273 A	274 Z	275 M	276 D	277 O	278 E	279 B	dhw	■	■

LIME-A, OHIO; LEEM-A, PERU

For many years, befofe there were Russian-language reference aids, the final authority on the pronunciation, usage, and meaning of any Russian word was the late Juliana M. She told you how every Russian word was *supposed* to be pronounced, how it was *supposed* to be used, and what it was *supposed* to mean. If anyone dared to say, "but they pronounce it..." or "they use it to mean...," she would angrily say, "They! the Soviets! they have bastardized the language! those peasants aren't speaking Russian! they're speaking Soviet jargon!" But what could you do, if there was only one oracle in town? You'd have to consult it! So people would find themselves asking MIss M. to render solomonic decisions, asking questions like "How do the Russians—not the Soviets—pronounce it" Is it Semipalatínsk? Or is it Semipalátinsk? Miss M. would answer, "Well, the name of the city comes from the Russian word *palâta*, meaning 'tent.' The name of the city means 'city of seven tents.' Hence the correct pronunciation is Semipalátinsk." (Smirk on face of disputant A—"I told you so!"; scowl on face of disputant B—"I know I've heard Russians—not Soviets!—say Semipalatínsk!") "However," Miss M. continues, "I used to know a man who came from Semipalátinsk, and *he* used to pronounce it Semipalatínsk."

The same kind of fight used to rage around the name Murmansk. Everyone in the United States knew the name at the beginning of World War II, because it was the northern port with the icefree harbor, where, before America was officially in the war, American convoys of merchant ships delivered all those lend-lease shipments that Soviet historians don't seem to recall that the Soviet Union ever got. And everyone used to pronounce it Murmánsk. So imagine the linguists' surprise to hear that "the correct pronunciation of Murmánsk is Múrmansk."

But doubt persists between the Murmánsk and Múrmansk factions. Finally the bastardizers of the pure Russian language publish a dictionary of pronunciations of personal and place names, worldwide, for the use of Russian radio and television announcers, movie directors, and the like. Naturally the Murmánskers and the Múrmanskers race one another to the M pages. There it is, sure enough—"Múrmansk." But then, in a more leisurely moment, reading for fun the introductory remarks on "How to use the dictionary," one of the disputants reads that "the pronunciations given in this book are the standard ones for use on nationwide radio and television. No indication is given of certain nonstandard or local pronunciations, for example, the local mispronunciation of Murmánsk instead of Múrmansk." That's the problem! People don't even know how to pronounce the name of their own hometown!

— From "Twelve Language Anecdotes in Search of an Author," by Arthur J. Salemme, retired

P.L. 86-36

AIT (U) [redacted] R94

This article is classified ~~SECRET~~ ~~HANDLE VIA COMINT CHANNELS~~ in entirety.

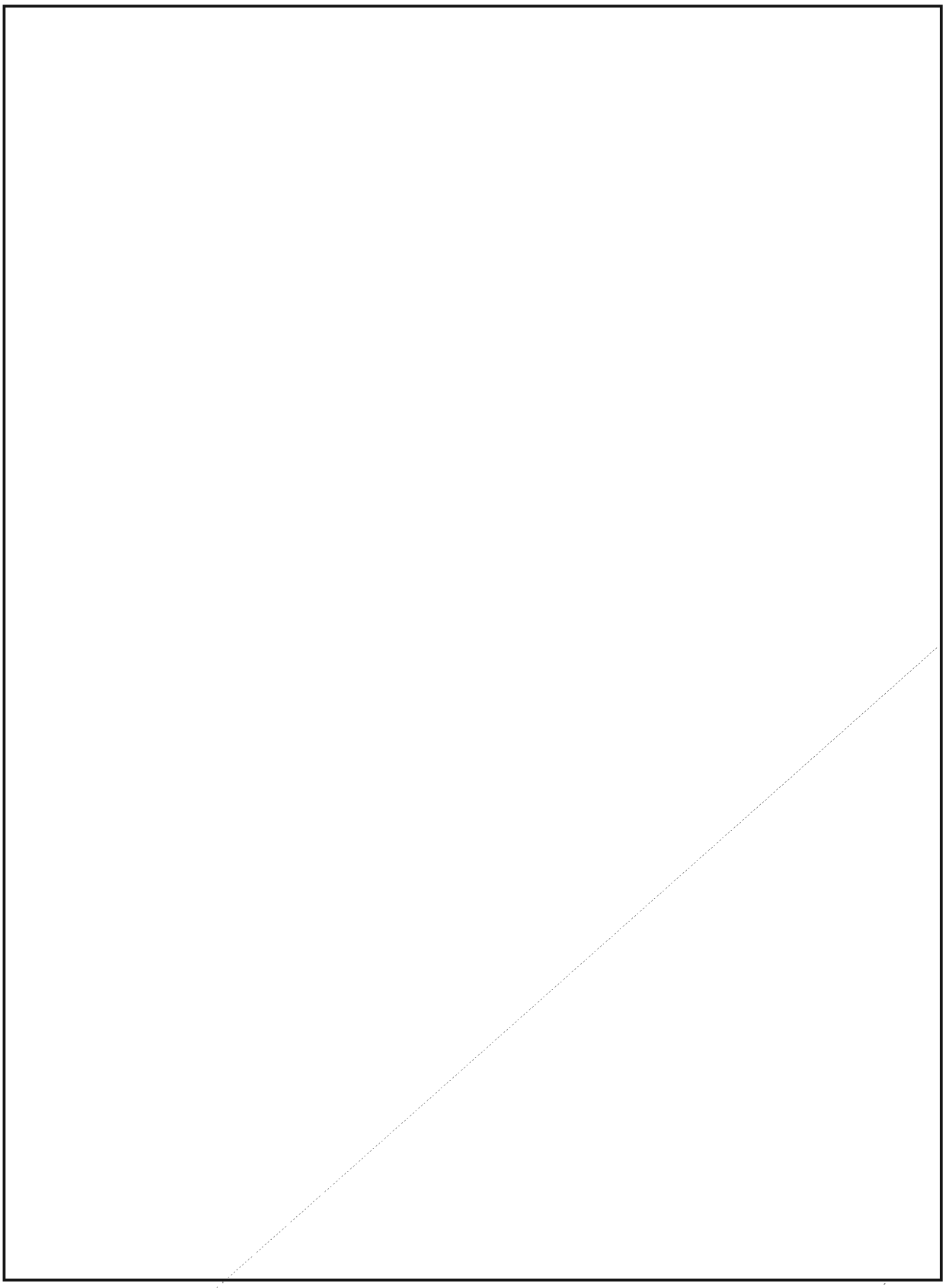
Advanced Identification Techniques (AIT) provide a means for identifying transmitters by their unique RF characteristics. In this article [redacted] provides a brief summary of the history and present status of AIT, as well as a glimpse into its future. dhw

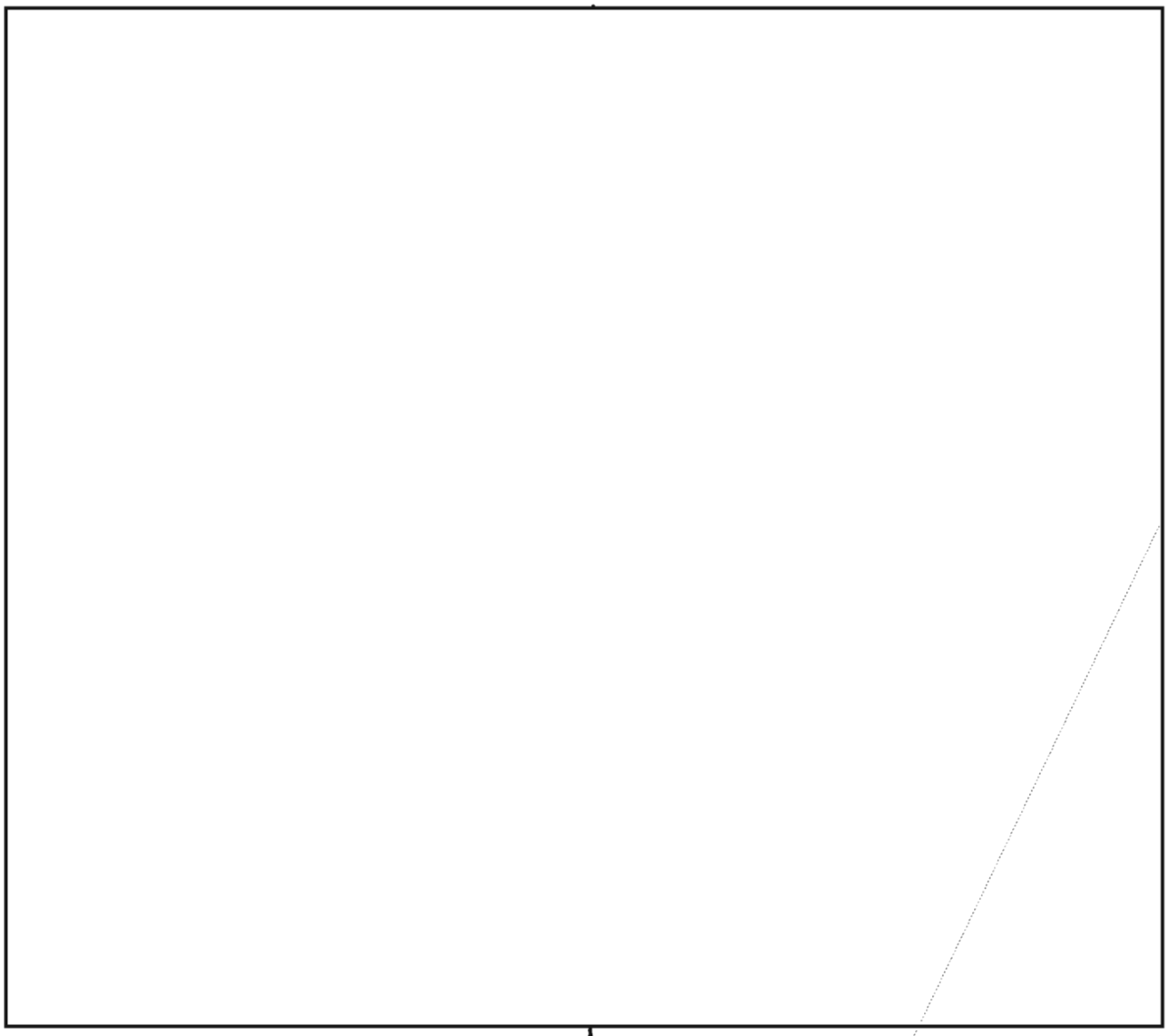
An early aspect of AIT is Radio Fingerprinting, a technique for examining the characteristics of transmitters to determine unique aspects that will allow these transmitters to be identified when seen on another occasion. [redacted]

[redacted]

[redacted]

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





(UNCLASSIFIED)

Answers to GEOGRAPHIC TRIVIA
(From Page 8)

EO 1.4.(c)
PL 86-36

- Frequent travelers to the Eastern Shore, who are convince that Delaware must be the flattest state, are almost ocrrect. With a high point of 442 feet (near Wilmington), Delaware comes in second. But first place goes to Florida, which soars to a high of 345 feet (in Walton County, in the western panhandle). Incidentally, when Washington, D.C., becomes a state, it will not displace Florida. Washington's altitude high, near the intersection of Wisconsin Avenue and River Road, is a surprising 410 feet. The highest low is in Prowers County, Colorado (3350 feet), where the Arkansas River enters the state of Kansas.

- Surprise! The most populous state capital is Indianapolis, with 725,077 inhabitants. It is followed by Honolulu (705,381) and Phoenix (664,721). The ten largest non-capitals are (in order) New York, Chicago, Los Angeles, Philadelphia, Houston, Detroit, Baltimore, Dallas, San Diego, and San Antonio. Washington, D.C., ranks twelfth. (These figures are from 1975 Census Bureau estimates; preliminary information from the 1980 census shows some changes to this ranking.)

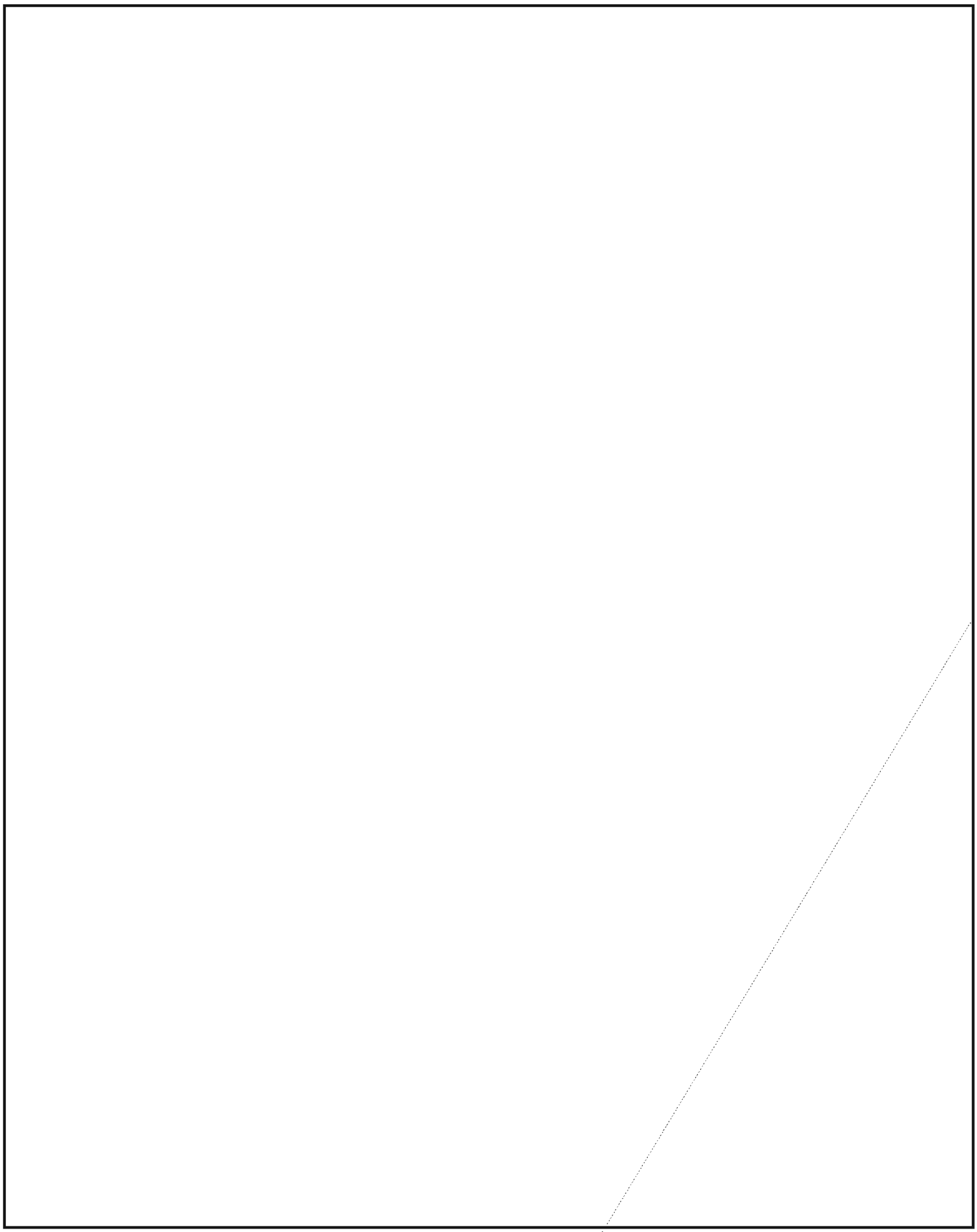
(UNCLASSIFIED)

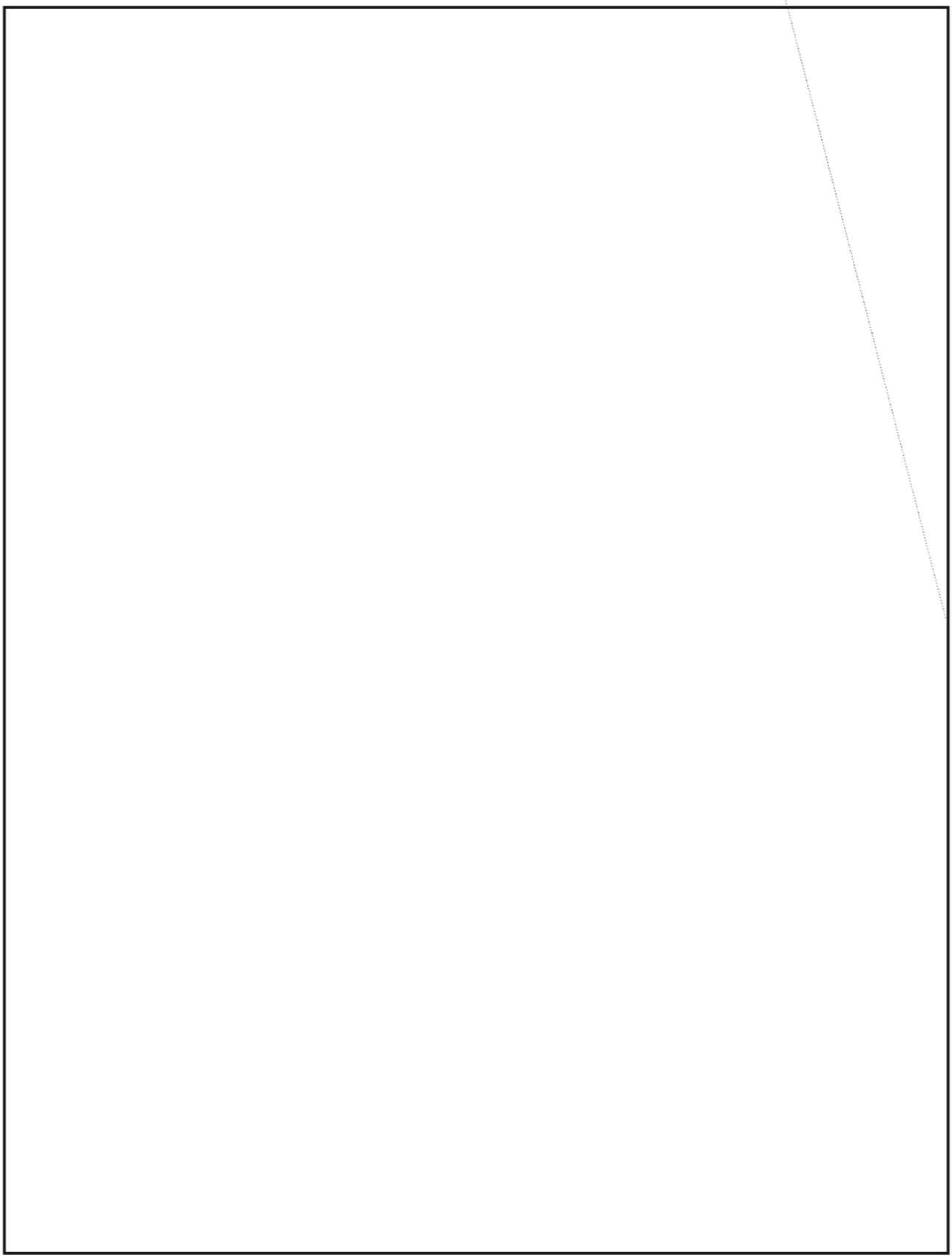
SOVIET C^3 (U)

This article is classified ~~TOP SECRET UMBRA~~ in entirety

P.L. 86-36

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





(UNCLASSIFIED)

What to Do About "FANX"

[redacted] A04 P.L. 86-36

Back in the sixties a coworker who lived in Linthicum used to drive to Ft Meade via Elkridge Langing Road, near Friendship Airport. Along that route construction had begun on a site described as "the future location of the Baltimore– Washington Science – Industry Center." "Very interesting," he thought. "Maybe in a few years I can bring my kids down here to tour some of these scientific and industiral institutions." How surprised he was when it was later announced that the occupants of the site, which was to become known as Friendship Annex, or FANX, were to be part of NSA's growing population, including him.

From the very beginning, the acronym FANX caused a pronunciation problem. My own unscientific investigation reveals about a fifty-fifty split among Agency employees. One half is convinced that FANX is a one-syllable word, pronounced FANX, while the other half, composed of equally intelligent people, pronounces it with two syllables—FAN-ex.

(This is somewhat parallel to the difference of opinion on how to pronounce the term "DIRNSA." In this case, my informal poll shows that a decided majority of Agency employees prefers the two-syllable DIRN-sa. But there is a stubborn minority that insists that it is a three-syllable word: dir-EN-sa. But I digress.)

I hope that members of both FANX pronunciation camps were as disturbed as I was several years ago, when the Credit Union put out a flyer, aimed at those of us who were working at the airport installation. This flyer hailed us as "Dear FANXITES!"

FANXITES?

The word made us sound like some kind of insects that come out of the woodwork. Didn't they know what we preferred the more elegant term FANXEANS?

If you didn't know the derivation, you could imagine that it was actually PHANX-EANS. Now isn't that a lot more classy, almost Grecian sounding. FANXITES, my foot!

Of course, since the state of Maryland changed the name of the airport from Friendship to Baltimore– Washington (or BWI), the term FANX has become obsolete. This has bothered me for quite a while, and I have tried to come up with a name that is more appropriate. Believe me, it hasn't been easy.

You can't do much with BWI to make a pronounceable acronym. I rejected "Airport Annex" since it doesn't tell which airport (National? Dulles?).

You could go the way of some area wags, who tried some time ago to popularize the term "Baltington" to describe the megalopolis that surrounds the B - W Parkway. Personally, though, "Baltington Annex" has about as much appeal as "FANXITES."

How about "Parkway Annex?" No, it sounds too much like a tacky motel.

I tried picking out another prominent landmark in the area. The biggest thing around, after the airport, is the Westinghouse plant. After experimenting with the firm's name and abbreviation, the best I came up with was "Compound W." Somehow that wasn't quite it.

I had almost given up, when I stumbled onto the solution. The annex is located in the South Linthicum area. So what would be more fitting that "South Linthicum Annex?" Accurate and descriptive, but not very exciting, you say? Not to worry. Like Friendship Annex, it is bound to become more popularly known by its contraction: SOLINEX.

The cash award I expect to receive from the Suggestion Program for this contribution will be donated to the Civilian Welfare Fund. The satisfaction of having solved the FANX problem will be reward enough for me.

(UNCLASSIFIED)

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

HELP WANTED (U)

Tom Engle, Senior Linguist in A64, with his tongue only part way into his cheek, offers this prospective recruiting flyer to any Agency element which might wish to use it.

N O T I C E N O T I C E N O T I C E N O T I C E N O T I C E

CHALLENGE ! EXCITEMENT ! ADVANCEMENT ! FUTURE !

All of this can be YOURS with a career in A6 ! Apply today!

IF YOU HAVE A DEGREE IN

Aeronautics	History
Chemistry	Law
Engineering	Mathematics
Finance	Medicine
Geography	Physics
Geology	Science

IF YOU HAVE BEEN EMPLOYED AS

Cartographer	Political Analyst
Communications Specialist	Politician
Computer Specialish	Test Pilot
Mechanic	Truck Driver
Newsman/Broadcaster	Weather Forecaster
Photographer	Xray Technician

OR IF YOU HAVE

Been an admiral
Been an astronout
Been a general
Built a rocket
Engaged in international trade
Launched a satellite
Managed an industrial enterprise
Negotiated an arms agreement
Planned military operations
Run a railroad
Served as a diplomat
Served on a Military Advisory Group

APPLY TODAY ! DON'T DELAY !

QUALIFICATIONS***	POSITION OFFERED
5 of above subjects	GG-5/7 TRANSCRIBER TRAINEE
10 of above subjects	GG-9/11 JOURNEYMAN TRANSCRIBER
20 of above subjects	GG-12 SENIOR TRANSCRIBER
ALL of above subjects	GG-13 SENIOR LINGUIST

*** NOTE: ALL APPLICANTS MUST BE QUALIFIED RUSSIAN LINGUISTS.

~~TOP SECRET~~