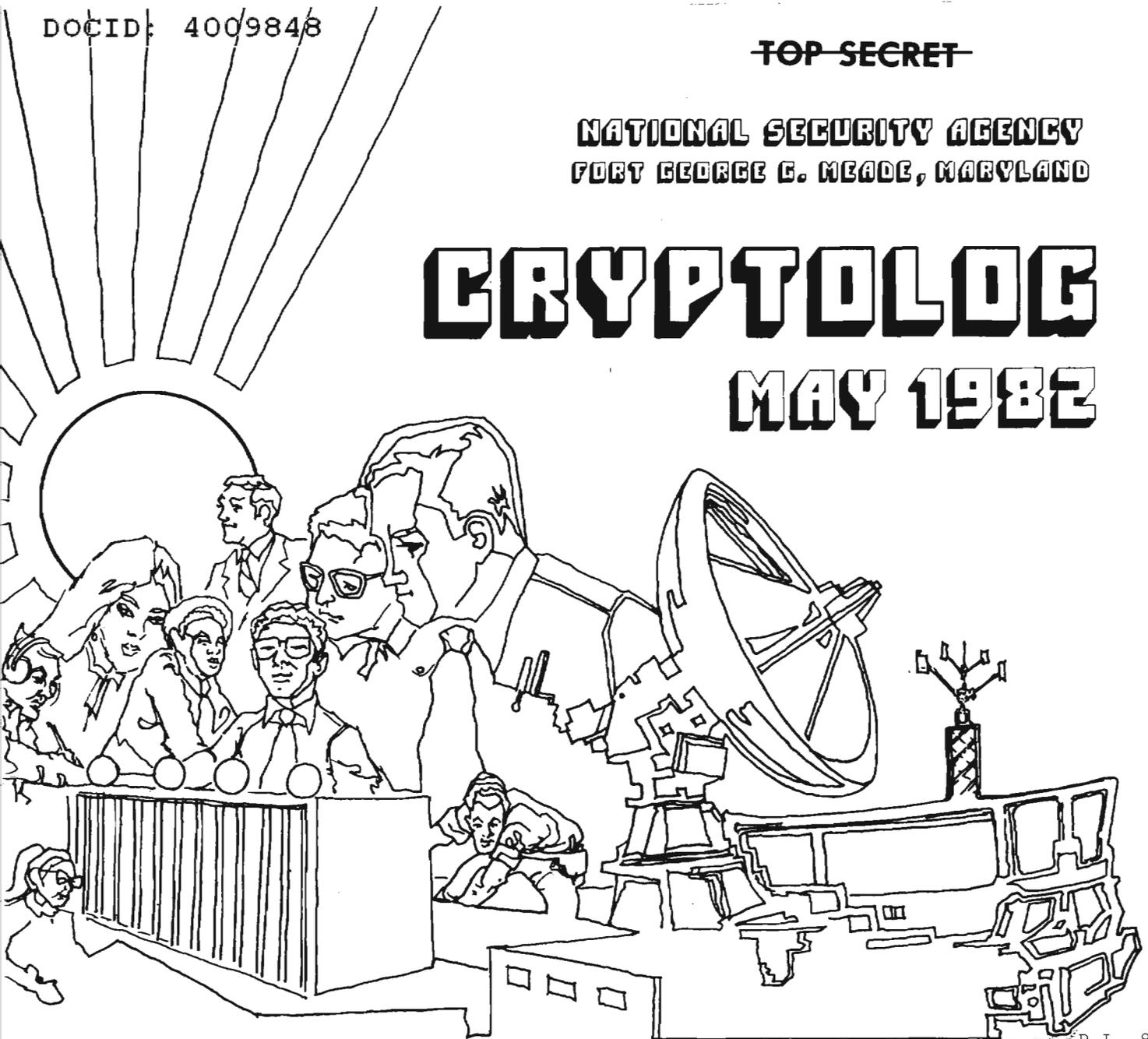


~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MAY 1982



P.L. 86-36

THE NSA INFORMATION DESK: "NO COMMENT" (U).....	[REDACTED]	1
THE MICRO REVOLUTION: ARTHUR YOUNG STUDY (U).....	[REDACTED]	5
COMMENT (U).....	[REDACTED]	9
HUMAN FACTORS: DATA GATHERING (U).....	[REDACTED]	11
HOW DO WE SPEND OUR DAY? (U).....	[REDACTED]	16
FULL OR BROAD SPECTRUM LIGHTING (U).....	[REDACTED]	14
CRYPTOLOG NUMBERING (U).....	[REDACTED]	14
TRUE BASE: TWO TALES (U).....	[REDACTED]	15
MAILBOX (U).....	[REDACTED]	21
PUZZLE (U).....	David H. Williams	22
A HISTORY LESSON (U).....	[REDACTED]	24
IS THERE AN OLD CROW IN YOUR FUTURE? (U).....	[REDACTED]	28
BUST ANSWER (U).....	[REDACTED]	29

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 10 May 2012~~

CRYPTOLOG

Published by Pl, Techniques and Standards

Editorial

VOL. IX, No. 5

MAY 1982

PUBLISHER

[Redacted]

BOARD OF EDITORS

Editor-in-Chief.	[Redacted]	(8322/7119s)
Production.....	[Redacted]	(3369s)
Collection.....	[Redacted]	(8555s)
Cryptanalysis.....	[Redacted]	(5311s)
Cryptolinguistics.....	[Redacted]	(5981s)
Information Science.	[Redacted]	(3034s)
Language.....	[Redacted]	(8161s)
Machine Support.	[Redacted]	(5084s)
Mathematics.....	[Redacted]	(8518s)
Puzzles.....	David H. Williams	(1103s)
Special Research.....	Vera R. Filby	(7119s)
Traffic Analysis.....	Don Taurone	(3573s)

For subscriptions
send name and organization

to: CRYPTOLOG, P1
or call [Redacted] 3369s

To submit articles or letters
via PLATFORM mail, send to

cryptolg at barlc05
(note: no '0' in 'log')

Many years ago, when the Pennsylvania Turnpike first opened, there weren't any other "super highways" as we now know them, and I was fascinated by how much easier and faster this new road was than any other route through the mountains. But after a while, as I travelled that road, it seemed as though I always managed to encounter at least two tie-ups, caused by repair crews whose work closed one lane or otherwise slowed the flow for miles.

One day, it occurred to me that these repair crews were always there, somewhere. After all, as the old punchline goes: everybody's gotta be somewhere. And where else would road repair crews be?

It seems to me that there may well be a similar principle working around here, except that it involves moving. No matter where I look, somebody seems to be moving. A lot of people seem to be "movers," involved in the mechanics of moving. Is there a PERT chart somewhere, with planners pondering the question of what to do with "the movers" during that empty period in FY88? After all, every mover has to be somewhere.

In the good old days, when we got to the new location after a move, we just took out our pencils, looked for a good place to put the pencil sharpener, sat down, and started to work. But now that everything is inside a computer somewhere, it doesn't seem to work quite that way. I wonder what it costs to move, in terms of lost hours, equipment repair, delayed reconnection of terminals, etc.

Maybe someone has all this under control, and from his vantage point, it all looks very orderly and smooth.

wed

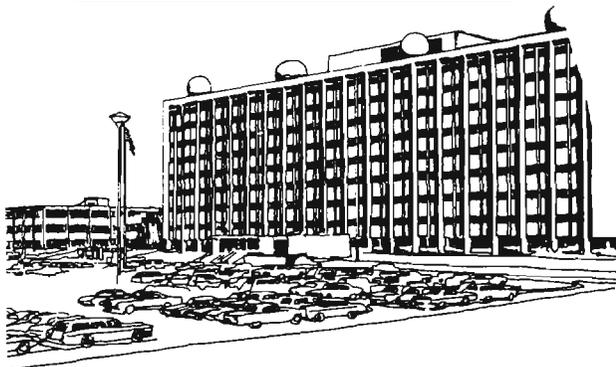
The NSA Information Desk:

by



Q44

P.L. 86-36



NO COMMENT (c)

Have you ever wondered what working for the NSA Information Affairs Division is like? How can there be such an organization when, normally, ~~(FOUO)~~ the only answer NSA gives to questions from the outside world is "No Comment"? Do people like Jack Anderson, David Kahn, and Mike Wallace ever really call NSA? Do other people call and say they are Richard Helms?

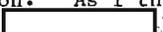
~~(FOUO)~~ Working on the NSA Information desk has been most interesting, sometimes frantic and hectic, usually busy, but seldom dull. I hope you will enjoy reading about some of the routine and exciting things that have happened over the past eleven years.

~~(FOUO)~~ Since many of you may not be aware that NSA has an Information Affairs Division, I'd like to begin with a brief history of how it all got started. In November 1965 NSA Director, LtGen Marshall Carter, USA, named  as "NSA Liaison Officer to the Assistant Secretary of Defense for Public Affairs." Initially, this was a part-time role; however, in December 1966 the position became full-time and the title changed to "Public Information Officer." In July 1967 the position was physically and administratively moved to the Director's Executive Office, and in July 1973 the title was officially changed to "Public Affairs Officer."

~~(FOUO)~~  who was this Agency's first and only "Public Affairs Officer,"

selected me as his assistant in June 1971 to succeed  who wanted to work part-time. At that time, I was working in the Counterintelligence Division of the Office of Security. In June 1973 a clerical assistant billet was added, and in August 1973 the Public Affairs Office (PAO) became D3 and relocated to the fifth floor.

~~(FOUO)~~ In January 1974 a decision was made by the Management Council to disestablish the PAO as a separate activity and to place the responsibility with the Chief, D41 (Policy Staff). As a result of this decision, Mr.  was given an assignment in the M organization, the clerical billet went to the Executive for Staff Services, and I remained with the PAO function. It may seem that the Public Affairs Office had a short life; however, in spite of losing the title, the function was neatly tucked away within the Policy Staff, and today the Information desk is alive and well.

~~(FOUO)~~ So much for history. You're probably still wondering what is really accomplished here in the Information Affairs Division. As I think back, I have often wondered if  hired me because he knew I could honestly respond to media calls with an "I don't know" or "No comment." Never having been exposed to the Operations or COMSEC functions has been a blessing on many occasions. More on telephone calls later.

~~FOR OFFICIAL USE ONLY~~

~~(FOUO)~~ The Information Affairs Division supports the Director, Deputy Director, and senior officials. One of the first services initiated was the news clipping service. In the beginning (1972), with limited staff (me) and reproduction facilities, the news clippings were provided once a day to DIR, D/DIR, and DC/CSS. Each day five newspapers (N.Y. Times, Wall Street Journal, Washington Post, Baltimore Sun, and Washington Star) were reviewed and items of interest clipped and formed into a mini-newspaper. In addition, the daily DoD Current News and CIA news clips were reviewed, as well as Time, Newsweek, U.S. News and World Report, Federal Times, and others, on a weekly basis. In recent years, additional requests have been received for this service and we are now able, with increased staff and a better repro machine, to provide copies twice each day to DIR, D/DIR, Chief of Staff, and all key component chiefs.

TELEPHONE CALLS

~~(FOUO)~~ Calls from the media are received in the Information Affairs Division and, depending on the requests, our responses vary. Camera crews from various media have been authorized to come and take pictures of the NSA buildings. We make the appointments and arrange for the crews to be met by a representative of the Office of Security who accompanies them as they photograph. Some callers ask for interviews with the Director or other seniors. Generally, because of our desire to maintain a low profile, interviews are not granted; however, Admiral Inman made a few exceptions. One such interview was given to Deborah Shapley of Science Magazine on the subject of public cryptography.

~~(FOUO)~~ Several years ago, I was surprised indeed to answer a call from Mike Wallace who was asking permission to photograph the Enigma machine for a segment on intelligence which was being prepared for "60 Minutes." Arrangements were made to accommodate his request.

~~(FOUO)~~ Jack Anderson's staff has called on several occasions asking for comments on subjects relevant to NSA. Also, ABC, NBC, and CBS have made frequent calls asking NSA to confirm stories about the Agency when we happened to be mentioned in the news. It is always amusing when they preface their call with "I am sure you won't make any comments, but...." Usually they are correct.

~~(FOUO)~~ Back in 1979 I received a call from a Baltimore Sun reporter who had learned that

NSA was seeking to acquire a couple of buildings at Aberdeen Proving Grounds for "warehousing." She wanted to know precisely what the storage space would be used for and, while I really didn't know, I told her it would probably be used for storing furniture, old records, etc. She asked more questions and became a little "pushy" so I commented that "I'd rather not discuss it further, because it was really a nothing move anyway." When I came to work the next morning and found that she had quoted me verbatim, I was a little shook until I heard [redacted] laughing about the "nothing move."

P.L. 86-36

~~(FOUO)~~ Last year some information was provided to the Baltimore Sun in response to an inquiry they had made concerning our recruiting efforts. The Director approved a release stating that we would be hiring over 1,000 new employees primarily with engineering, language, and computer skills. The publicity was good but the Recruiting Office was literally exhausted from answering over 500 calls in a matter of a few days.

~~(FOUO)~~ Of the 75-80 media calls that are received during a year, most are legitimate. However, we have our share of "crank" calls. There are a few that have made good "in house" stories for many years.

~~(FOUO)~~ I recall a man who insisted on speaking with the Director (Adm Gayler) who was then away on TDY. He then asked for Dr. Tordella by name and stated that it was urgent that he speak with him--that the information he had was critical and timing was of utmost urgency. I sensed that he was "disoriented" but not being sure what to do, I called Security. This man made about ten phone calls to NSA and actually flew down to BWI, rented a car, and came to NSA. He was interviewed by a Security Officer. The following weekend, this individual was arrested in New York and held under \$500,000 bond on charges of paying \$1,000 to a secret service undercover agent to assassinate President Nixon.

~~(FOUO)~~ Then there was the caller from North Carolina who called on successive days and said that he was "hooked up to the NSA computers." I tried to explain to him that this would not be possible, but he was very persistent. Finally, on about the third day, I told him that he was no longer hooked up--that everything on this end had been unhooked. I haven't heard from him again.

~~(FOUO)~~ Another very business-like caller

~~FOR OFFICIAL USE ONLY~~

identified himself as Richard Helms. He was calling from New York and stated that he was working on a special NSA project. He needed some money and wanted it sent to him as soon as possible--he even gave what he claimed to be an NSA account number. Thinking the call to be legitimate, the respondent (not me this time) dashed into the Director's office and related the story, only to return with a red face. The caller was really an imposter.

~~(FOUO)~~ One disgruntled citizen called and asked some specific questions about NSA. I explained to him that the information was not releasable, which made him angry. He said he was a taxpayer and had a right to know. Just before he realized his efforts were fruitless, he said he intended to make a citizen's arrest. Sometimes having a name like isn't all bad.

~~(FOUO)~~ All calls that come to the switchboard for the Director are first screened by the Information desk. Some of the callers are very insistent; however, after a few questions it usually turns out that they simply need the Agency address, or have been turned down for a position and want to know why. Occasionally, the caller will be a Congressional or White House staffer and, of course, these calls are immediately transferred to DIR's office. On the other end of the spectrum, an angry man called recently. It seems he had been selling eggs at one of the gatehouses and that the FPS had asked him to leave. He asked about the people who sell flowers and was told that they were the exception to the rule. His last statement, after expounding upon his rights, was "If they can sell their flowers, I can sell my eggs." I suggested that he write a letter of request, but to date we haven't heard from him.

DO WE GET ANY 'CRANK' LETTERS?

~~(FOUO)~~ Do we get "crank" letters! Many are received each year and, again, depending on what they say (if that can be determined), we either forward the letter to Security, answer it ourselves, or simply file it. Some are amusing, others aren't.

~~(FOUO)~~ One of the most amusing letters was from an individual who identified herself as the "Commanding General United States Marine Corps" and she had the business cards to prove it. She sent a mailgram (three pages) which expounded on her background and told how, during World War II, she had made secret trips to the Kremlin and to Hitler's headquarters for

President Roosevelt. Her photograph later appeared in the 3 March 1976 issue of the Baltimore Sun, as one of the "fringe candidates" who had requested that her name be placed on the ballot in the Maryland primary election as a presidential candidate.

~~(FOUO)~~ Another classic letter was from a lady in Denver who claimed that she hadn't received her share of the Rockefeller estate, which she believed to be at least \$150 million. She later made a request under the Freedom of Information Act and, in our response, we advised her of our fee-charging policy. We asked her to pay half of the fee prior to initiating the search. The next thing we knew, she was in the lobby at Gatehouse 1, waiting to pick up records that we might have. She called our office, and we just told her again that we couldn't assist her until we received a certified check--which we never got.

P.L. 86-36



SOLUTION TO NSA-CROSTIC No. 39

"Thou Swell, Thou Witty," by D. Hart

"I know Larry had tremendous love and respect for Richard Rodgers. I believe that the love was mutual. After all, it is not remarkable that they split up after twenty odd years, but that they endured and survived during those years."



~~(FOUO)~~ You've read in the NSA Newsletter about some individuals seeing some mice in various areas. Well, I doubt that anyone has ever seen a "holographic mouse" except our friend in Florida who has sent several letters. She writes that "whoever beamed a holographic mouse out of the glass jar on the kitchen counter across the sink and over to the refrigerator got it almost perfect." She contends that someone is playing pranks on her and has been since she applied for work here. Also, she has been experiencing ear beeping, and she has been used in the development of an early warning system for VIPs which involves ear buzzing and beeping signals that can be accompanied by physical retaliation against attackers or even the VIP if he/she doesn't follow orders.

~~(FOUO)~~ We also get some "not-so-crank" letters from amateur cryptographers who send in their own designed cryptosystems for evaluation. One individual attached part of his system in a sealed envelope with a statement which read:

"Before opening the attached envelope, let it be agreed that I have not relinquished my rights to this system. If this stipulation cannot be met, please return it to me by Registered mail."

Needless to say, the package was wrapped, addressed, and returned by Registered mail.

~~(FOUO)~~ Another man called one day to inquire about a letter he had written. He didn't want to give me his name but finally consented after I convinced him that it would be impossible to search for his letter if I

didn't have a name. We couldn't find the letter, so he mailed us another copy. The letter was sent Registered mail, with no return address. It wasn't signed, but attached to the letter in a sealed envelope marked "Confidential" was his name and address.

~~(FOUO)~~ In addition to preparing news items and responding to letters and telephone calls, the Information Affairs Division approves the release of all unclassified information in accordance with NSA/CSS Regulation 10-11. This includes all résumés, reports of co-op students, newsletters (including "unclassified" CRYPTOLOG articles), talks to be given at seminars, etc. To give you an idea of the volume, in 1981 approximately 480 requests were processed.

~~(FOUO)~~ Today, the Information Affairs Division is part of the Policy Staff (Q4). We have a staff of six people and work as a team processing Freedom of Information Act (FOI) and Privacy Act (PA) requests as well as manning the Information desk.

~~(FOUO)~~ Many times, NSA employees have assisted us by bringing to our attention the fact that NSA has been mentioned on the news or that they have read an article where the Agency has been mentioned. We appreciate this assistance because it enables us to keep the senior-level people better advised. Occasionally, an NSAer has been called by a reporter who has acquired the name from some source. When this happens, the only recourse is to refer the call to the Information Affairs Division, and we will see that the proper response is made. The telephone number is 688-6524. We are here to support all of NSA and are happy to assist when we can.



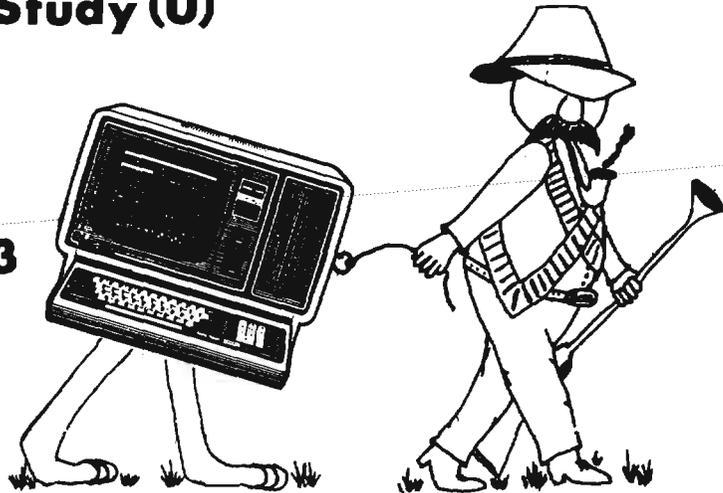
The MICRO Revolution: Arthur Young Study (U)

Comment

by



P13



P.L. 86-36



Recently the Directorate of Data Automation of the Department of Defense initiated a study with the consulting firm of Arthur Young and Company to explore the potential impact of low cost computing on the Department of Defense (DoD). This article presents excerpts from the Executive Summary of the study issued by Arthur Young and Company, followed by my comments.

"In the last several years rapid advances have been made in almost every area of information technology, and these trends have far-reaching implications for the management of this technology in the Department of Defense.... The Reagan administration, the Department of Defense and military strategists throughout the armed services are grappling with the problem of identifying the most efficient and effective applications for scarce resources.... But, because of technological advances, some investments which appear to be costly are, in fact, cost-effective. Understanding when an investment is justified is an intricate process requiring both technical and management expertise.... The Department of Defense has in the past assumed a leadership role in responding to the demand for information. DoD has acquired the most efficient information processing technology available and has developed the professional staff essential to maintain this technological capability. Information processing technology, however, is the most rapidly changing industry

in the market today. The cost of logic circuits continues to drop approximately twenty to thirty percent per year, while the cost of solid state memory decreases approximately thirty to forty percent. New capabilities at reduced cost are being announced almost every day.... The current options available for processing information are widely varied. They include new equipment, new operating and application software, and new management tools.... The options are so varied, and their potential management, technical, organizational and personnel impacts are so extensive, that they may obscure the ultimate goal of identifying the information processing approach that will lead to the lowest cost for groups within DoD and for the department as a whole.... DoD believes that of the emerging technologies, the low cost computing systems available today and in the future will have the strongest impact on DoD of all ADP technology trends.... At the summary level the most important trends are as follows:

- ★ Hardware capabilities are increasing significantly with improved processing speed and reliability. For example, memory size is increasing while costs drop at the rate of thirty to sixty percent per year. Storage capacities are also increasing rapidly.
- ★ The quality of printers and of a variety of input/output devices is increasing substantially, while the cost is decreasing.

UNCLASSIFIED



- Improved quality of work from data entry activities to reduced effort and time required to generate and review documents, and finally to more rapid and accurate decision making.
- More timely response to the information processing needs of users throughout DoD.
- Cost savings through replacement or enhancement of obsolescent information processing equipment.
- Cost savings through automation of labor-intensive, and therefore increasingly expensive, manual procedures in areas where automated support has not been cost-effective in the past."

- ☆ Advances in telecommunications technology are making local networks attractive.
- ☆ The major improvements in color, graphics, and end-user orientation are accelerating the expansion of computer applications.
- ☆ High quality software packages are widely available for applications from general accounting and word processing through individual management decision support tools.
- ☆ Most importantly, the large base of equipment sold is creating compelling economic incentives for vendors in the software market. The number of desktop microcomputers installed is projected to grow from approximately one million in 1981 to five million by 1985. The incentives in the microcomputer software industry will keep pace with this unusual growth."

"While the technological trends are important for the ADP professional to monitor, it is the management implications of these trends that are of greatest significance to DoD executives and policymakers.... The changing technology has ... created both new opportunities and new issues that demand the attention of senior management.... The opportunities presented by changes in information processing technology may be summarized as follows:

"These opportunities support major objectives of DoD and of the current administrations: to increase productivity while cutting or containing costs. The opportunities encompass an additional benefit: the integration of state-of-the-art information processing technology will increase the attractiveness of DoD for the most talented managers and ADP professionals entering the job market...."

"During our review of technology trends, we determined that the computer equipment and associated software available at the lowest cost, the microcomputer systems, are generating a vast new market among users who have little or no ADP technical background. Microcomputers, offered at costs well below the delegated procurement authority in DoD, are readily available to this market group. These new users can benefit from the technical expertise and management perspective of ADP professionals if an effort is made by DoD to anticipate problems and highlight opportunities.

A variety of interrelated factors contribute to our expectation of widespread DoD acquisition and use of microcomputers. Among the most significant of these factors are the following:

- User frustration with the largely centralized ADP technology and services provided within DoD is caused by time delays both in processing information and responding to new or changed application

UNCLASSIFIED

UNCLASSIFIED

requirements. This frustration is intensified by the inability of users to customize programs to their local needs and the difficulty they experience in attempting to communicate their needs to data processing personnel.

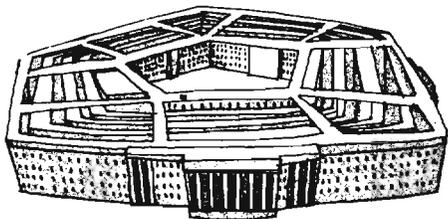
- This problem is further heightened by the high level of use and old age of the average DoD computer equipment. The capabilities and services provided by this old equipment fall far short of the capabilities found on many of today's low cost computers....
- The low cost computing technologies, particularly microcomputers, are therefore especially attractive to users who see them as a means to reduce their problems with the centralized ADP support found in the government today. A parallel benefit is offered to ADP professionals who have been struggling to meet demand with a perpetual shortage of qualified programmers. The user orientation of the microcomputers may help to mitigate the projected major personnel shortage in DoD.
- During the next few years, budgetary limitations and personnel constraints or cut-backs will become a reality for DoD. Managers will be expected to face the challenge of decreased resources for day-to-day operations and staff functions.
- Low cost computing technologies offer significant opportunities for enhancing productivity to meet this challenge. Microcomputers, especially, are viewed as a means to eliminate a wide variety of time consuming manual procedures and inefficient automated procedures.
- Because of the relatively small investment of resources required for the initial purchase of a microcomputer system, the amount of time required to repay the investment in terms of personnel hours saved is small. As technology costs decrease and personnel costs increase, investments in low cost technology become increasingly attractive.
- Contributing to DoD users' frustration with existing information processing technology and services is their perception of the high quality and powerful capability available to them at a low cost in systems that have been designed especially for

operation by end-users. Microcomputer technology vendors have identified these users as a new and potentially profitable market segment. They have designed both their systems and their marketing techniques to appeal to non-technical users, as well as ADP professionals. In doing so, they have developed systems which require little or no interaction with computer programmers and operators.

- The microcomputers, furthermore, are increasingly reliable, well-documented and supported. The combination of high quality and user-friendly orientation may be expected to add to the attraction of low cost computing technology within DoD for managers, military analysts and administrative personnel.
- DoD should anticipate the impacts of a combination of user frustration and the availability of low cost alternatives that appear to be ideal solutions to users who, in the past, have been unaware of many ADP options.
- Today's users are more receptive to computer technology than they have been in the past.... Along with even a rudimentary understanding of what low cost computing technology can do for individual users comes acceptance and a feeling of control. Familiarity, acceptance and control by the end-user will encourage widespread acquisition within DoD."



UNCLASSIFIED



"We anticipate that the combined impact of these four interrelated factors will be widespread acquisition and use of microcomputers within DoD. Along with opportunities that these low cost systems present, however, come some critical issues which DoD management needs to address."

"... The most critical issues are those that have not been encountered before in managing ADP resources. Also critical are the more familiar issues which have taken on a new slant with the changes in technology.... Specifically, the issues of greatest concern for DoD senior management are:

1. Control of Acquisition and Use

- The issue of control begins with the fundamental question of whether control over the acquisition and use of microcomputers systems is desirable, or whether it will serve only to obstruct the initiative of managers to find innovative, cost-effective applications for the new technology. If control is desirable, the most appropriate level for control needs to be identified.

- DoD has, thus far, consciously proceeded without formal, centralized control over low cost computers. This policy has been adopted to encourage

experimentation, which will serve both to clarify the real potential of microcomputers and to highlight potential pitfalls.

- Ultimately, some degree of control is necessary to ensure compatibility of resources and to promote sharing through networking or integration with mainframe systems. Control will also be necessary to ensure compliance with data security and privacy laws and with applicable federal procurement regulations and Public Law 96.511.

2. The role of microcomputers in relation to mainframes and minicomputers

- ADP professionals in DoD will need to develop expertise in the process of identifying which functions are most appropriately handled on a mainframe, a minicomputer or a microcomputer. Microcomputers can be used as stand-alone processors for applications with limited input/output device requirements and limited volume processing needs. They can be used as remote terminals in a dial up mode with a mainframe to provide decentralized access to centralized systems. Microcomputers can be used in small clusters supported by a mainframe, or in super clusters where portions of the processing burden are down-loaded to remote processors connected to the mainframe.

- The clarification of the most effective roles for microcomputers in relation to mainframes and minicomputers will require extensive ADP technical expertise. It will also require a senior management perspective on organizational and personnel issues within DoD.

3. Application Areas and Sequence for Introduction

- The areas where microcomputers can be used in DoD are numerous. They include enhancement of traditional data or word processing functions and development of new applications to support individuals directly in management or decision making activities.

UNCLASSIFIED

- The management issue which results is in identifying where the systems can be used most effectively.

4. Pace for Introduction and Integration

- A key concern for DoD management is the pace at which low cost systems are introduced. A rapid pace involving a large number of applications over a broad range of user groups may cause failures and widespread disillusionment and implementation of incompatible systems. On the other hand, an extremely slow pace will cause dissatisfaction among users who are eager to install the systems immediately and a delay in achieving higher degrees of cost-effectiveness.

- The careful selection of pilot sites, where strong and technically capable proponents of microcomputers are available to lead the implementation effort, may prove most effective.

5. Roles and Responsibilities of Users, ADP and Word Processing Professionals

- Perhaps the most demanding management issue presented by microcomputers is the development of new roles and responsibilities. The traditional division of duties will continue to change with the introduction of this new technology. Users will work more directly with computers. ADP professionals may find significant roles in decentralized support activities spread throughout the user community.... There is a need initially to encourage and eventually to require the acquisition of appropriate microcomputer expertise among users, ADP and WP professionals.

6. Support Structure

- The installation of a significant number of microcomputer systems raises several important management issues for DoD in the area of support structures. The primary question to be answered is, how will the systems be acquired, maintained, and operated.

- Currently, low cost computers are generally being acquired individually or in small numbers. If DoD continues this process, the department faces the potential problem of acquiring large numbers of incompatible systems--causing interfacing problems and increasing the cost of training. At issue is the question of whether a central acquisition support structure could acquire these units at volume discounts, while achieving increased compatibility. However, a concern is raised that this support structure may slow down the acquisition process and possibly lock DoD into older technology.

- The support function also extends to the availability of software packages which are being purchased individually in increasing numbers. An issue arises concerning whether DoD should enter into multi-site package arrangements or whether it should develop and distribute its own software packages."

"The preliminary analysis of low cost computing trends, impacts and implications has identified some major opportunities for DoD. It has, in addition, made it clear that several significant management issues need to be addressed in order to take full advantage of the opportunities."



UNCLASSIFIED

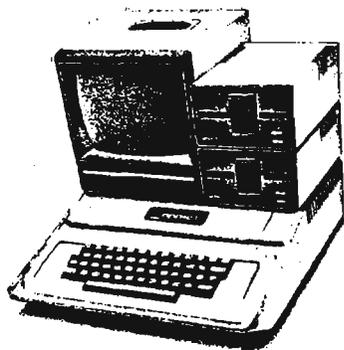
 THE MICRO REVOLUTION: A COMMENT
by P13

P.L. 86-36

For the past several years P13 has been experimenting with personal computers for cryptanalytic applications within DDO. As a DDO technical staff, our efforts have been directed toward helping the analyst who is still doing the great bulk of his work by hand.

In our efforts to investigate the use of this new technology for DDO applications, we have encountered some of the possible scenarios suggested by the Arthur Young study. Users tend to be frustrated by the response that they receive from the ADP service organizations and are therefore quick to pick up on the possibilities offered to them by the personal computer. It is friendly and they have immediate control over it, which leads to great acceptance by even the most unsophisticated (in terms of ADP) user. We can see, therefore, that the potential problems and pitfalls which the Arthur Young study refers to, as well as the many opportunities, are real and must be dealt with.

As a result of our experiences in the personal computer arena, I believe that we are in the middle of a processing revolution which will greatly enhance the capabilities of all analysts, especially those doing labor-intensive tasks. Also, there are opportunities offered to the user of a personal computer in other areas, such as word processing, data base systems, and information management.



Since the inception of our efforts to investigate the potential uses of personal computers for cryptanalytic applications in DDO, we have become very aware of the large variety (which seems to grow larger every day) of personal computer hardware and software which is available from commercial sources today. In attempting to acquire some of these tools for the DDO analyst, we have encountered some of the problems which the Arthur Young report alludes to, including the necessary acquisition lead time--which leads to user frustration and to the procurement of obsolete technology--and the service problems which occur due to the diversity of equipment.

Nonetheless, we in P13 agree wholeheartedly with the Arthur Young study's conclusions. Personal computers are here to stay, and they offer DDO and NSA managers many unique opportunities. However, they also present many new managerial problems. At the present time I believe that the issue which requires immediate attention from NSA management is:

How can personal computers be acquired, maintained, and operated without stifling the initiative and innovativeness of local managers?

I know that some of the problems foreseen by the Arthur Young study exist in NSA today. One of the many unanswered questions is how are we going to deal with them? I don't have answers to the questions raised nor am I sure that these are the only possible questions. But I am sure that NSA must deal with them soon.

As I see it, the major questions generated by the Arthur Young study are:

- ◇ what effect will this DoD concern for microcomputers and their use have on NSA, and
- ◇ how will NSA, and in particular DDO, deal with the revolution that has already begun?

Copies of the Executive Summary of the Arthur Young study are available from P13. A copy of the full report is also available. To obtain any of this information or to discuss personal computers and their use in further detail, please contact me.

HUMAN FACTORS:

- Data Gathering (U)
- How Do We Spend Our Work Day? (U)

by P13



P.L. 86-36



These articles were written a couple of years ago, after I returned from taking the Human Factors Summer Course at the University of Michigan. Since that time, I have been involved in a human factors experiment concerned with improvements to Transcribers' working environment, in the course of which extensive use was made of another electronic data entry device, the KAMAN Scientific Corp ADES "Electronic Clipboard." I hope to prepare a paper in the near future, describing the use made of this device, and the results obtained.

the use of hand-held electronic recorders which can be used to time and record observations, and then can be plugged in to a computer terminal or modem to transmit the data to a computer where software provided by the manufacturer analyzes it and sends back a display of results. The demo he gave us used a DATAMYTE electronic data collector (ELECTRO-GENERAL, Minnetonka, Mich.) and data was transmitted and analyzed via a TI "Silent 700" portable terminal.

A classic Time Study was defined as follows:

"the analysis of a job for the purpose of determining the time it should take a qualified person, working at normal pace, to do the job, using a definite and prescribed method. This time is called the standard time for the operation. Standard times are developed by adding up the times for each element of the work cycle."

(from Human Factors Newsletter 1-79)

For me, the most valuable feature of the human factors course (University of Michigan) was the coverage of methods for gathering and analyzing data, and design of human factors experiments. Paul Green, of the Highway Safety Research Institute at Michigan, gave a very interesting lecture and demonstration of methods for gathering data. This seems to me to be a crucial part of the problem we face in putting human factors concepts to work in our operations: how can we study the users, their tasks, and the work environment? How can we get the kind of hard data we need to design a better system for the user? Dr. Green introduced us to some "classic" industrial techniques, and gave us some "hands-on" experience in making a Time Study using a stopwatch and manual recording form. He also demonstrated

Dr. Green served as our Subject, while we actually tried to do a simple Time Study of a task involving inserting 5 screws into holes and screwing them home with a simple screwdriver. We were issued stopwatches, clipboards equipped with a little rack into which the stopwatch fitted, and a recording form. Then we determined the starting and stopping "rules" for each "element" within the work cycle. This involved finding visible benchmarks (e.g., "hand touches the first screw in the box," "puts screwdriver down on table,"

UNCLASSIFIED



In this kind of study, the observer marks down which of a set of predetermined activities the worker or machine is performing at some points during the total time he is observing (e.g., every 10 seconds) over a considerable length of time (several days or weeks). There are a number of automated aids for this kind of study also, for example, a beeper which signals the sampling times to the observer through an earphone, and a hand-held electronic recorder. A large number of computer packages have been developed for industrial applications, to look up standard descriptions of tasks and the standard work times established for them, and compute total times for a work cycle. These methods can be used for abstract modelling and simulation of work cycles before the actual tools or procedures have been implemented, basing their results on estimates from the standard values in the data bases available to the packages. The systems include standard times for such actions as "reach," "turn," "position," "move," etc., eye-movement times, and body, foot, and leg movement times. Some systems are specialized for office tasks and clerical tasks (these might be more relevant to many of our contexts than the industrial assembly-line kinds of tasks involved in most of the systems).

etc.) which an observer could reliably identify as he watched the worker. The actual observation was surprisingly difficult (the stopwatch took some practice in handling, and my reaction times were appallingly slow!). The advantages of the automated recording devices became abundantly clear in a hurry. In a real-life study, observers undergo extensive training with videotapes of workers performing an operation, until all observers can recognize and record all elements of the cycle to a predetermined degree of accuracy and agreement. A subjective decision has to be made about the pace at which a worker is performing the operation at a given time. Is it his normal pace? How does it compare to the usual pace of most workers doing the job? This obviously also requires a trained observer.

Another classic kind of data gathering procedure Dr. Green described was the Activity Sampling, or Work Sampling Study. This was defined as follows:

"The most global examination of what one or several individuals and/or machines are doing at many predetermined points in time for the purpose of finding out how time is allocated.... In its simplest form one records if the object observed is 'busy'."

I learned some interesting things about the real-life application of data-gathering techniques from a fellow-student, a management analyst from HEW, involved in design of a major interactive terminal system for the Social Security Administration. He described the method they had used to study the work of the intended users of the system, in order to provide a basis for design of the user dialog and functions the system was to perform. They were able to convince their top managers to release ten expert workers from different regions of the US, and assign them for several months full-time to work with the design team. The design staff taught these experts how to make flow charts, supplied them with manuals and all other information support files they normally used in their work, and asked them to create detailed flow charts of how they did their jobs. The procedures differed somewhat in different regions due to State laws, and the experts resolved or combined their differing segments of flow charts, working together. Unfortunately, this rather expensive description soon became out of date, and the design team is now faced with the task of revising it. Since top management is no longer willing to release experts from their regular duties and assign them to the team even temporarily, they will have to "go back to interviews and questionnaires" to get the needed data.

UNCLASSIFIED

HOW DO WE SPEND OUR WORK DAY?
(from Human Factors Newsletter 1-80)

In looking over my notes from the Human Factors Engineering Summer Course at the University of Michigan, I came across another bit of data which I thought might be of interest to you. It was part of a handout distributed to students by John D. Gould of the IBM T.J. Watson Research Center, Yorktown Heights, for his lectures on "Man-Computer Interfaces for Information Systems." His lectures were, in my opinion, among the best of the course. He presented a great deal of recent findings from his own research, and also provided us with excellent, up-to-date bibliographies, among them an extensive "Bibliography of Behavioral Aspects of On-Line Computer Programming." Any reader who would like copies of these can get them from me by calling me on x8845 or sending me a note.

Could described the results of a study of white-collar workers in offices. This study was an "Activity Sampling" study, using a data-gathering method I mentioned above. Trained observers recorded which one of a carefully pre-selected and defined list of activities office workers were engaged in at times sampled throughout the work day. Separate studies were made of secretaries on the one hand and "principals" (managers, professionals, technicians) on the other. While there have been many such studies of industrial workers, little is known about how office workers spend their working hours. I found the results of this study quite surprising. If anyone had asked me what I thought an office worker (non-secretary) did in a work day, I would have said something like this: "If he/she is a manager, he/she works at a desk writing and reading, attends a lot of meetings, and talks a lot on the phone. But if he/she is not a manager, most of the day is probably spent sitting at the desk reading or writing, with a few phone calls." Here is what the IBM researchers found (for "principals" only; unfortunately Dr. Gould did not include the findings for secretaries, which I would also like to see.):



How Principals Spend Their Time

- They are inside the office building only 75% of the time.
- They are in their work area only 50% of the time.
- They spend a surprisingly large portion of their time "communicating" as opposed to reading or writing, and an even more surprising proportion of their communicating is face-to-face talking.
 - ▶ All Communicating 40-50% of work time
 - face-to-face 30-35%
 - telephone 10-15%
 - ▶ Reading 10-15%
 - ▶ Writing 10-15%
- They communicate more by conversation than by formal memos or correspondence, and they engage in many relatively brief communications. Communication is relatively unstructured, non-repetitive, and involves constantly-changing content.
- Their day comprises an "unrelenting stream of varied activities," with an average of 16 interruptions of an ongoing activity in a day. Most meetings are unscheduled. Workers typically "juggle several tasks at once," and "have no idle time."

It is hard to estimate how similar these patterns are to the work activities of Agency professionals. It is my impression that the daily routine of many NSA "principals" (non-clerical personnel) involves far more valid, work-related face-to-face communication and walking around than we (or our managers) realize. I hope that we will soon have an opportunity to do some scientific activity sampling studies in NSA work areas, and gain some understanding of how our people spend their work hours. It is interesting to speculate about the effects of certain technological changes on these work patterns. How will a worker who is used to doing all that wandering around, impromptu meeting, juggling interrupts, and face-to-face talking adapt to activities centered around a computer terminal? Or a personal computing environment, that makes everything - even conferences - possible in his work area? I myself spend at least six out of eight hours at my computer terminal on most days, and I find that I create excuses to get up and wander around, hunt up someone to talk to, or start a (usually work-related) conversation with another worker nearby. I doubt that sending a message over the net or even teleconferencing would satisfy the need for a change of scene and for sheer physical movement that I feel after an hour or an hour and a half at the terminal.

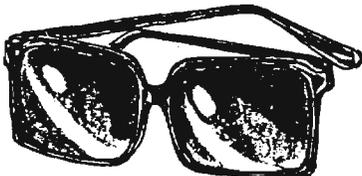
FULL OR BROAD SPECTRUM LIGHTING (U)
 by R335
 (from Human Factors Letter #3-81)

The terms "full-spectrum" or "broad-spectrum" lighting are new "buzz-words" that have been appearing in public print for the past few years. Currently, the terms are used to refer to lighting which closely resembles direct sunlight, including both the visible and non-visible frequencies (of the latter, at least the ultraviolet spectrum). An article in the Continental Airlines flight magazine EXTRA described Soviet claims of good results from the use of this lighting in office and work spaces (Ref 2). On the other hand, on-going US studies by the National Institute of Occupational Safety and Health (NIOSH) and the National Bureau of Standards have not only failed to duplicate the Soviet results, but in fact note a high risk of adverse effects (Ref 4).

(U) The primary risk from this type of lighting is due to the larger than normal amounts of ultraviolet that are emitted onto unprotected eyes and skin. The commercially-available "full" or "broad-spectrum" fluorescent lamps attempt to approximate sunlight by adding a chemical which fluoresces at the mercury-line wavelength of 430 nanometers. The result is a blue-colored light which is now considered by experts to create a risk of damage to human eyes called the "blue light hazard" (Ref 4). This commercially-available type of lighting appears to offer no advantage as a tool to improve the performance of VDU operators or other office workers, and in fact is likely to create a risk to visual health.

References

1. "Human Factors in Office Automation," W.O. Galitz, Life Office Management Association, Inc., Georgia, 1980, pp 68-70.
2. "Take it Straight from the Sun," EXTRA, Continental Airlines, May 1980, pp. 28-32.
3. "The Dual Function of the Eyes," John Ott, Southern Journal of Optometry, June 1979, pp 8-20.
4. Personal communications from Clyde C. Moss, NIOSH, and Dr. Robert Glass, National Bureau of Standards, 1981.



CRYPTOLOG NUMBERING (U)

~~(FOUO)~~ It is evident from your questions that some of you like to keep a complete file of CRYPTOLOG, and so for your use, here is a list of the issues, by volume, that have been published to date:

- Vol I, 1974 Numbers 1, 2, 3, 4, 5. (Aug-Dec, initial year).
- Vol II, 1975 Numbers 1, 2-3, 4, 5, 6, 7, 8-9, 10, 11, 12.
- Vol III, 1976 Numbers 1, 2, 3, 4, 5, 6-7, 8, 9, 10, 11, 12.
- Vol IV, 1977 Numbers 1-2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12.
- Vol V, 1978 Numbers 1, 2, 3, 4, 5, 6, 7-8, 9, 10, 11, 12.
- Vol VI, 1979 Numbers 1, 2, 3, 4, 5, 6, 7, 8-9, 10, (11-12 not used).
- Vol VII, 1980 Numbers 1-3, 4-6, (7-12 not used).
- Vol VIII, 1981 Numbers 1-3, 4-6, (7-9 not used), 10, 11, 12.
- Vol IX, 1982 Numbers 1, 2, 3, 4, 5 (this issue).

(U) Copies of most issues are available in limited numbers. Call Hal Smith (x3369s) or Wayne Stoffel (x8322s).

TRUE BASE: TWO TALES (U)

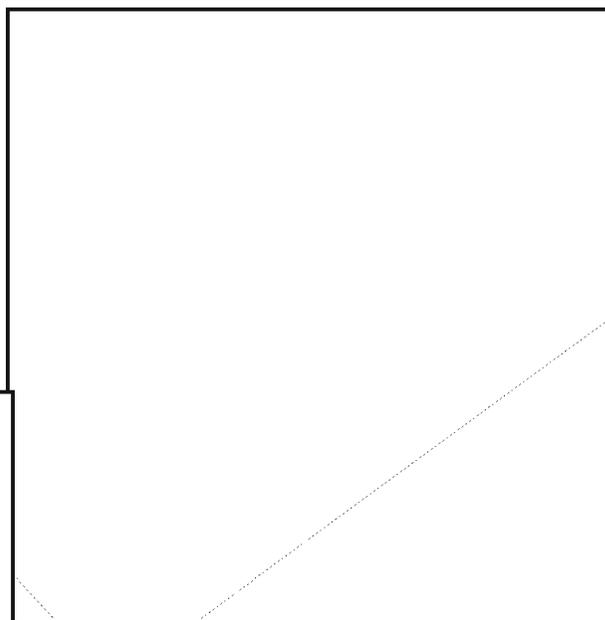
by PI

P.L. 86-36



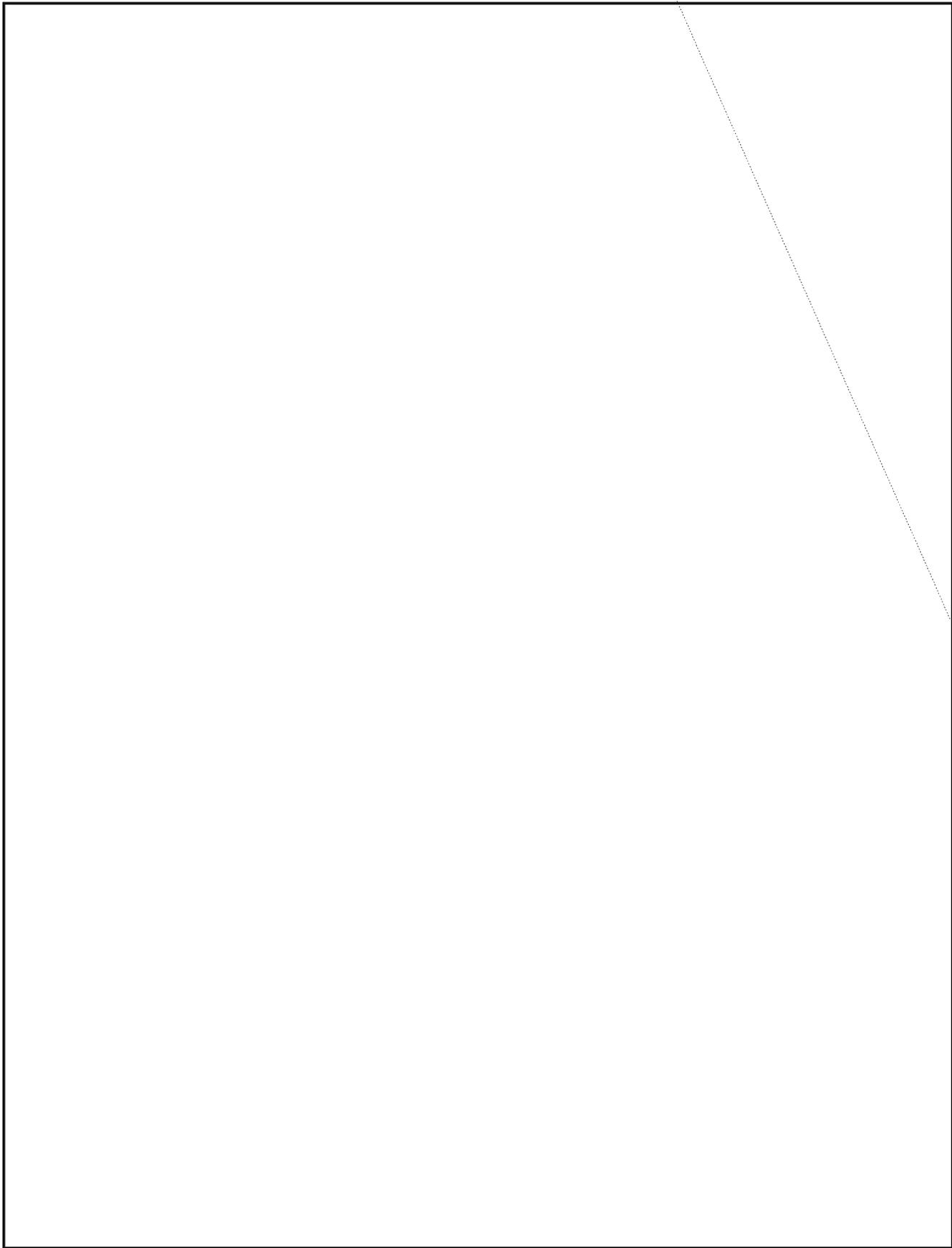
Both of these tales are true. Some of the details have been changed, but not necessarily to protect the innocent. They both have to do with the same thing: what happens to our knowledge about a target when we put one of its systems on true base.

First Tale



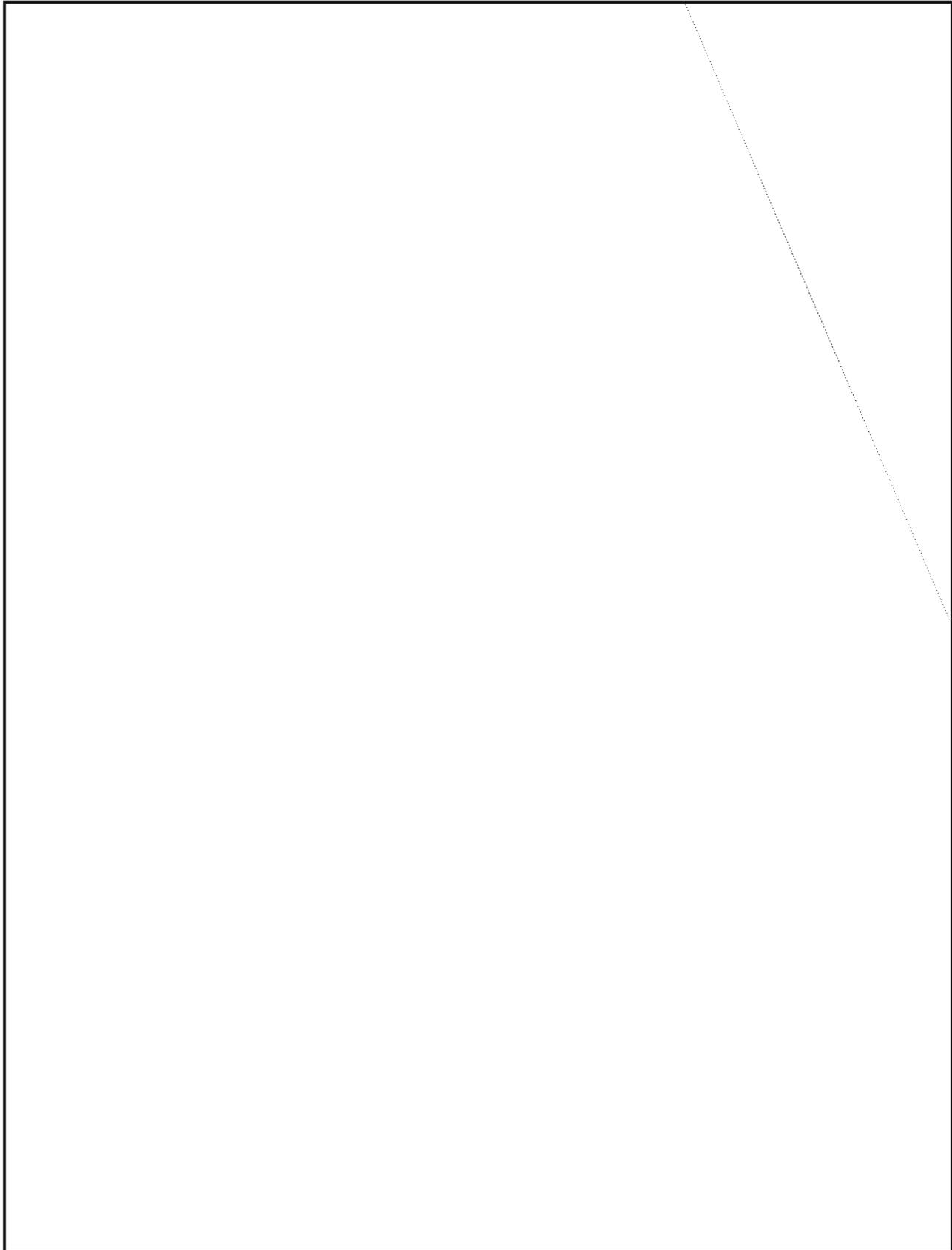
EO 1.4.(c)
P.L. 86-36

~~TOP SECRET UMBRA~~



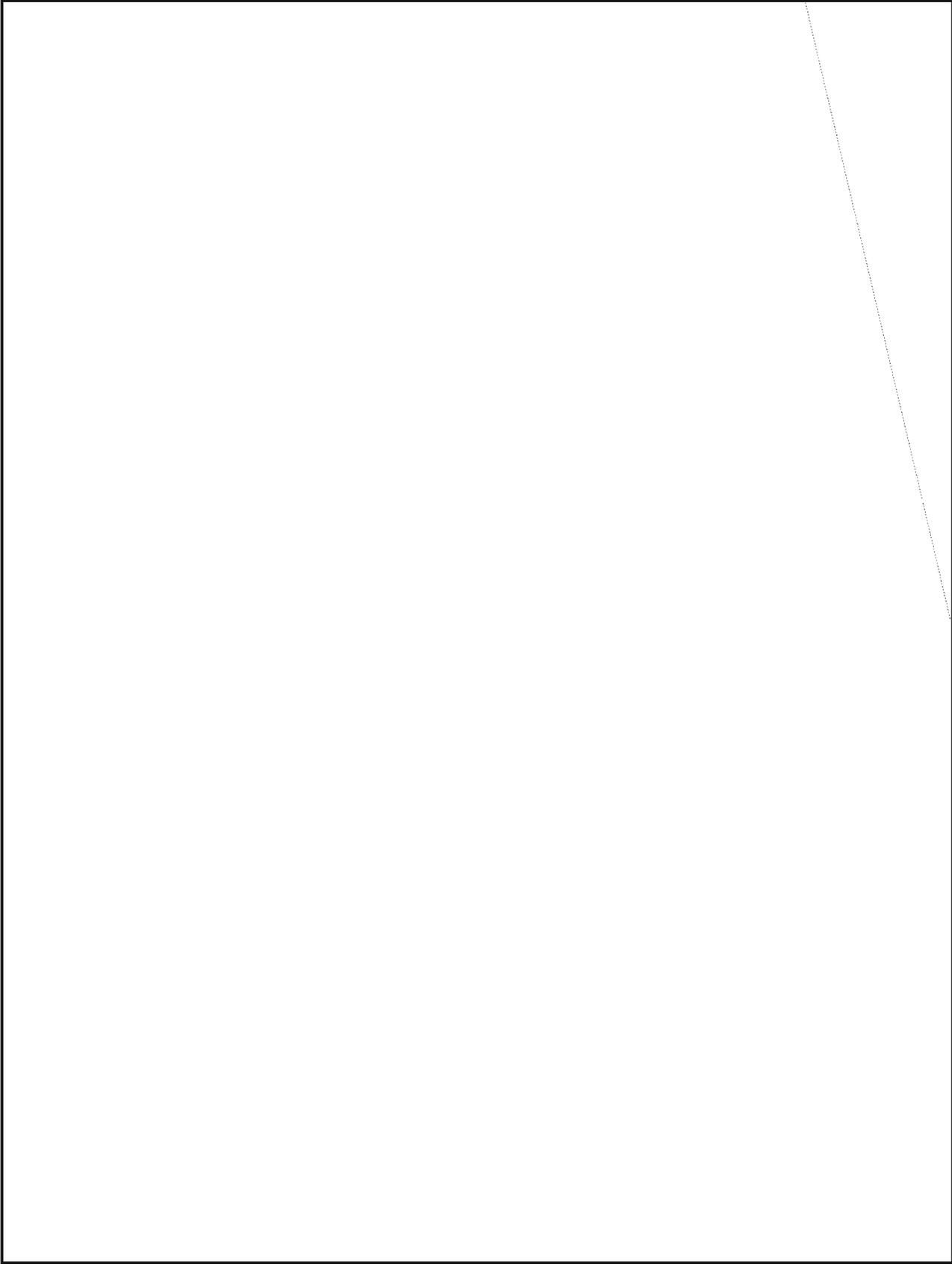
~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



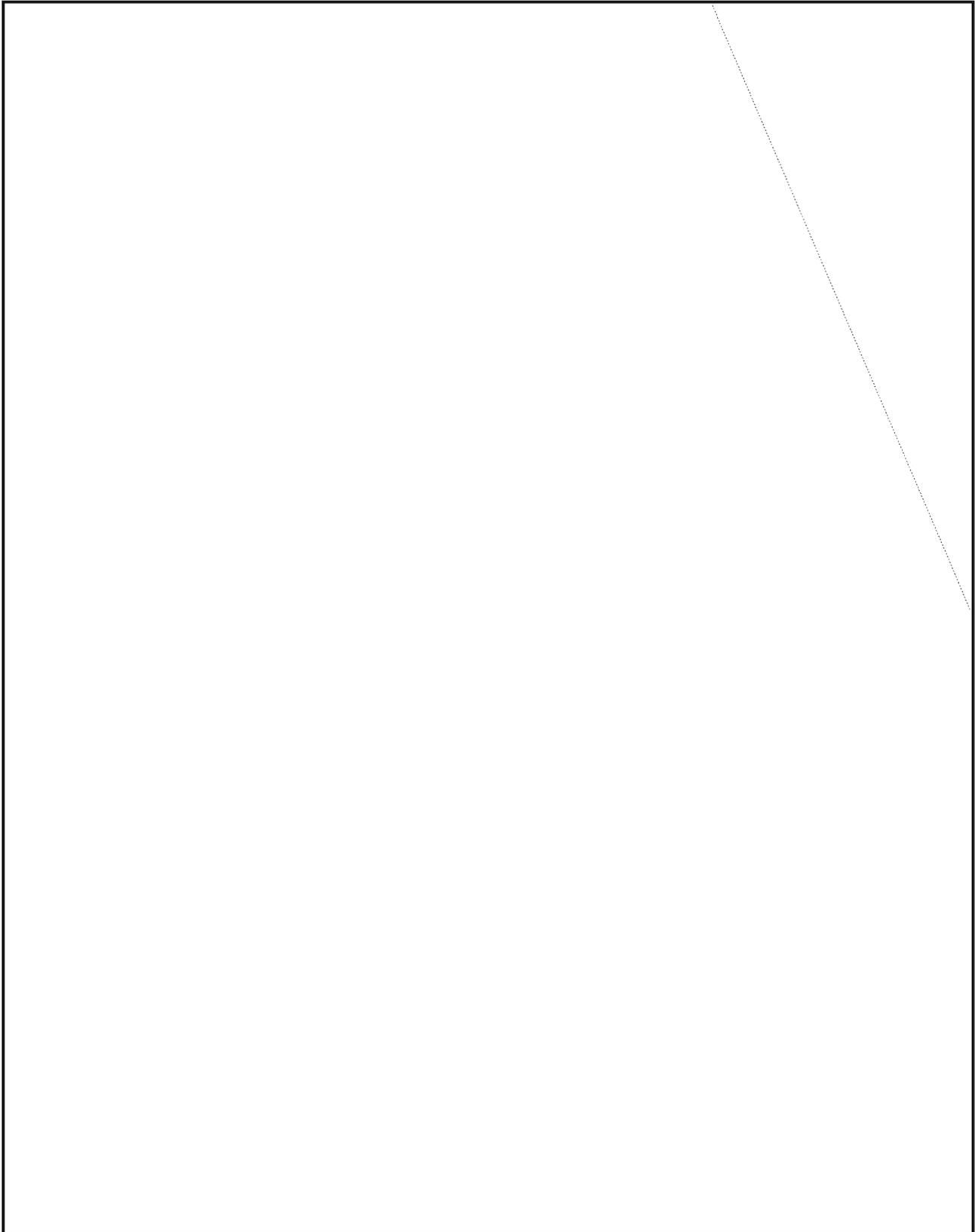
~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

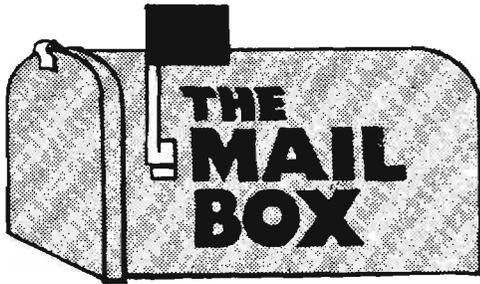


~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~



I must confess. I have worked at the Agency about 15 years and I still do not know how to spell the word "plaintext" (or words "plain text"). I have used various ruses in attempts to conceal my ignorance. For example, I have used "p/t" or "text" as substitutes, and I have tried to conceal "p/t" in hard to spell and/or hard to understand words and phrases. That is why my pulse quickened and hope arose when I picked up the March 1982 issue of CRYPTOLOG, and found on page one the words "plain text." Eureka. There the words are, in America's ultimate source on how to spell "p/t." (I haven't received a copy of NSATJ in a year, and believe it to be defunct.) If an official publication of NSA can not spell "p/t," who can? So, you spell it as two words. I quickly read and turned to page two to get verification by repetition. Alas--"plaintext" screamed at me--five times. Wait. Perhaps it may be spelled either way depending on some rule (e.g., one way if an adjective, another if a noun), I thought. Or perhaps the first spelling is just a typo--the editor did warn of such things at the very beginning. I quickly read on to gather more data. "p/t" appears three more times as one word, and twice more as two words. I could discern no rule. I could not believe three typos. Hope faded. I gave a laugh and resigned myself to continued illiteracy when I noticed near the end of page three a sentence beginning with a small letter.

Sincerely,

[Redacted]
A541

P.L. 86-36

From: jel at opman
Subject: programs
To: cryptolg at barlc05

P.L. 86-36

Read [Redacted] article on PINSETTER programs with some interest. I would suggest some sort of introductory comment noting that these programs will run on UNIX systems, but that the PINSETTER programs are not available on most UNIX systems. To my knowledge 'permute' is available only on [Redacted]. There is no arrangement with T3332 (UNIX Systems Support) to include these programs in a standard system.

In line with the above, I would suggest indicating which programs are standard agency UNIX programs (available everywhere) and which are PINSETTER programs for which special arrangements must be made.

[Redacted] d

From: dce at CARONA
Subject: Shell Game - "names"
To: cryptolg at barlc05
cc: dce

Hi,

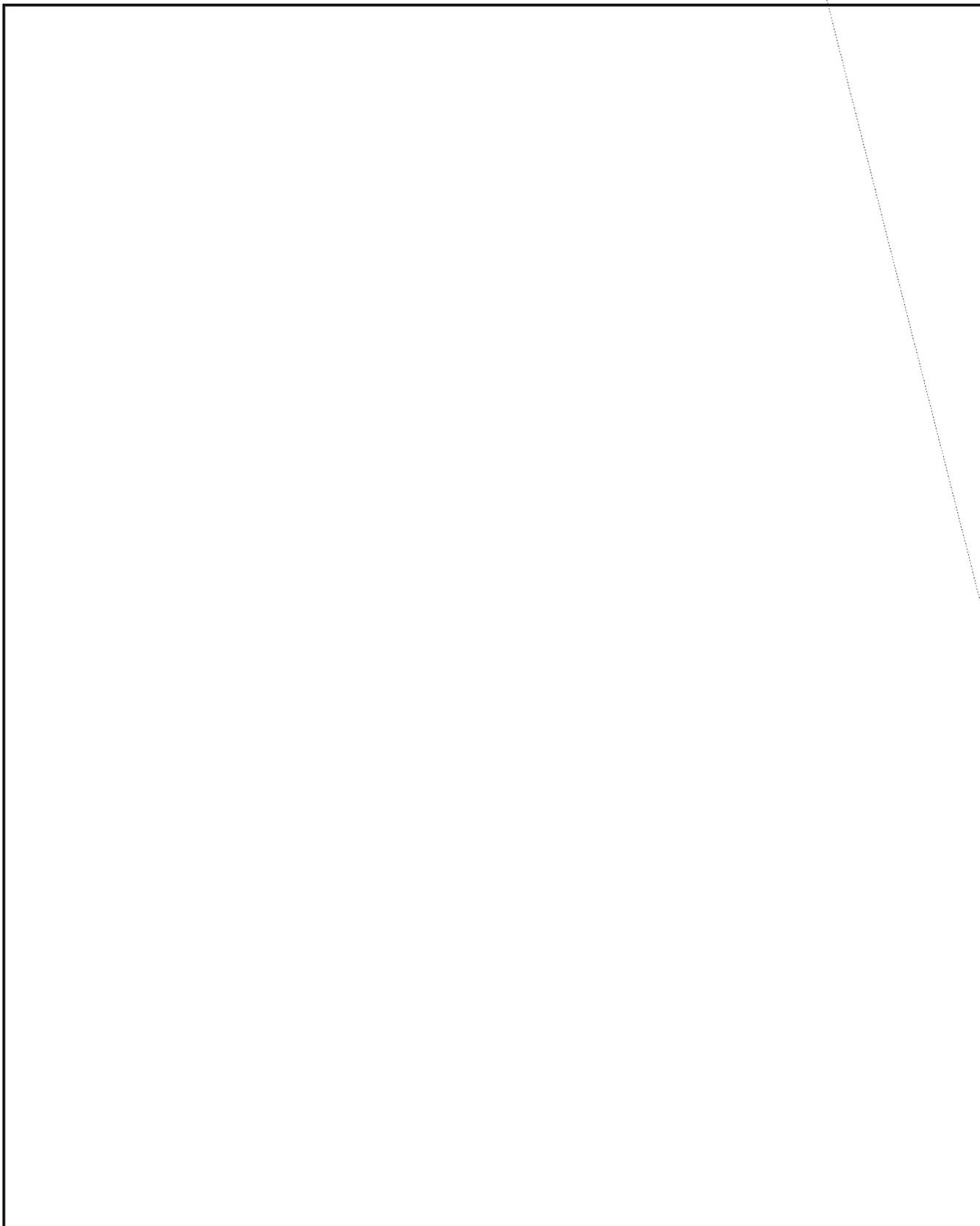
I just got my April 1982 issue of Cryptolog and noted with great interest the new feature Shell Game. I look forward to seeing this feature on a regular basis.

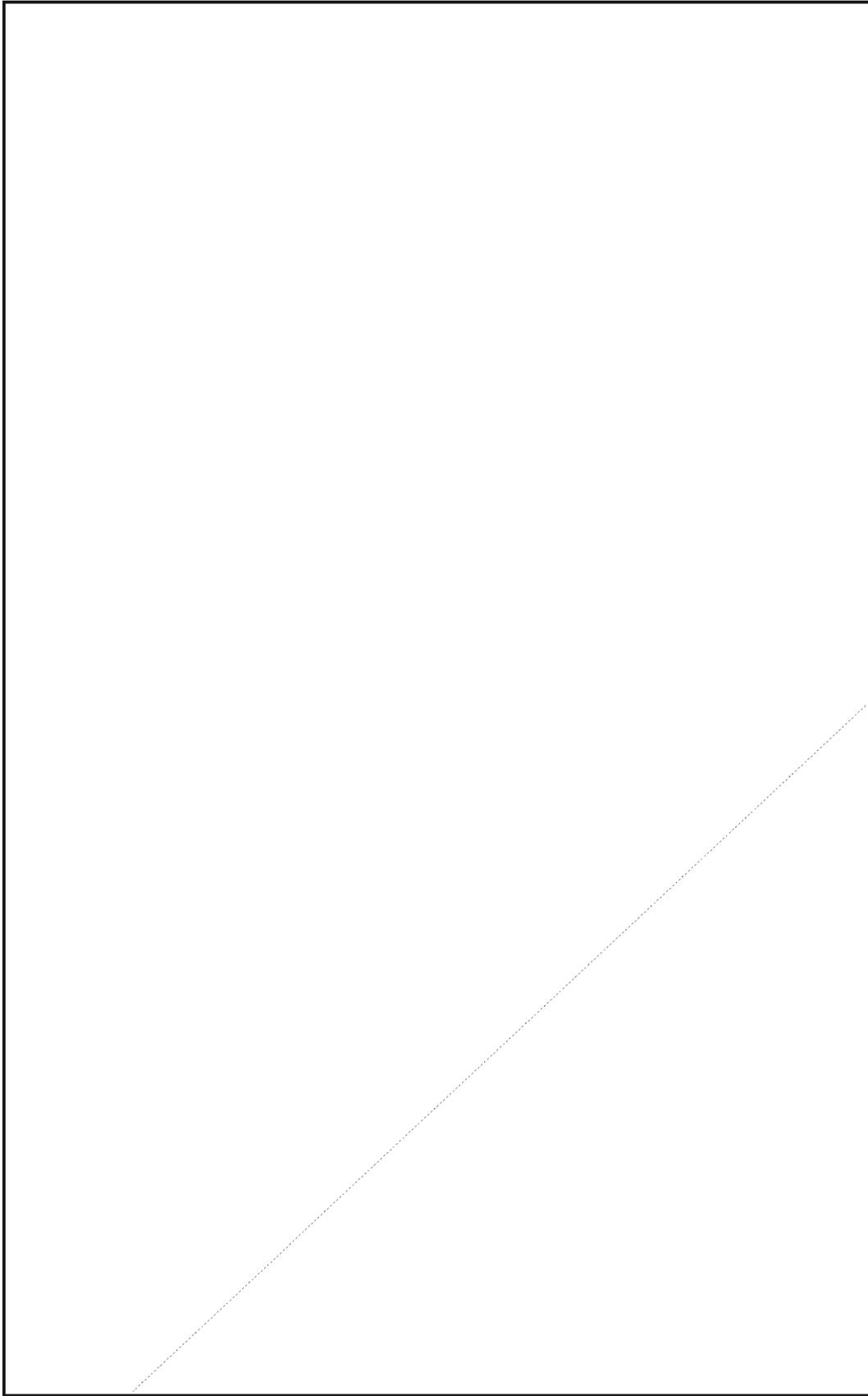
I like the names shell and have one very similar that I call whon. Frankly, I like the results of mine better and thought you might want to compare. Try this one:

```
who | reform +t8 | rp1 "~" "name " > whonames
sh whonames
rm whonames
```

Regards,

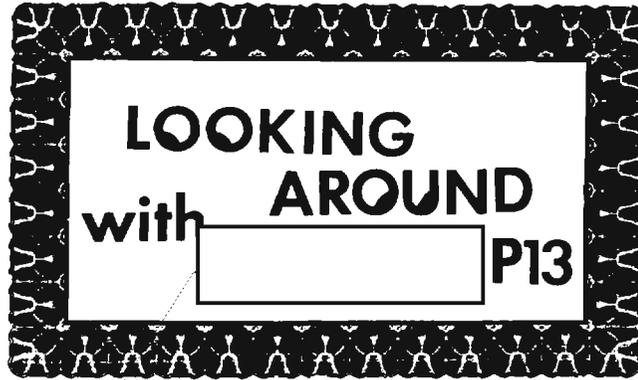
[Redacted]
T441,1181s (dce@carona)





NO PARTIALS IN

A HISTORY LESSON (U)



P.L. 86-36

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

By early 1942 British analysts ¹ had built up a favorable position in exploitation of Luftwaffe ENIGMA traffic, but a cascade of German ~~(TSC)~~ security changes, and new demands by the SIGINT recipients, forced a number of crises on the analysts, and incidentally forced the SIGINT effort to be more analytic and more tightly integrated.

This article is extracted from a briefing given by the author at the C.A.A. Conference, Fall 1981.

~~(TSC)~~ In 1940 GC&CS ² broke into ENIGMA traffic during the Norway campaign, but on 1 May 1940, the German Air Force (GAF, Luftwaffe) and German Army (GA) introduced a new indicator system which defeated the crypt-analytic methods. On 10 May 1940, Germany attacked in France and the Army came on the air on 3000 frequencies, which the BEF (British Expeditionary Force, the British Army in France) tried to cover with only 50 receivers. By 20 May 1940, the GAF RED key was solved and produced 1000 decrypts daily, but the intelligence was unused.

~~(TSC)~~ The "fusion" technique of combining decrypts and log readers' records showed that traffic analysis could help break ENIGMA. [redacted]

~~(TSC)~~ During 1940, all traffic analysis on ENIGMA communications was based on decrypts. The callsign system was unknown, but decrypts were not used to try to solve the callsign system. The German Army "Dog" book of 40,000 callsigns was captured in Norway.

~~(TSC)~~ In 1941, traffic analysis research found that the GAF used a "Bird" book for callsigns, similar to the GA "Dog" book, a system of 40,000 callsigns that had been captured in Norway; however, where GA frequencies were daily changing, the GAF frequencies were fixed. [redacted]

~~(TSC)~~ All messages had discriminants, so cryptanalytic sorting was based only on discriminants. Traffic analysis was not accepted in Hut 3 ³ unless based on decrypts. The aim of traffic analysis was to steer intercept, because of the shortage of receivers and operators.

~~(TSC)~~ The solution of the GAF callsign system (by Army analysts) completely changed the attitude of Hut 6 ⁴ toward traffic analysis, and initiated a policy of trying to read all traffic worth breaking. Hut 3 intelligence analysts wanted only 45 more receivers to cover ENIGMA communications, but Hut 6 traffic analysts held out for 240 more receivers to allow complete cover of Order of Battle and selection of traffic. A number of overlapping

EO 1.4.(d)

P.L. 86-36

EO 1.4.(c)

traffic analysis parties came into existence, each doing part of the traffic analysis mission, which was still undefined.

(TSC) By 1942, there were 40 new GA and GAF ENIGMA keys in use. The Quiet Room in Hut 6 found [redacted] and the Registration Room [redacted]

[redacted] This made efficient breaking and exploitation possible, despite the fanout of the key families.

(TSC) A reorganization of BP (Bletchley Park, wartime location of GC&CS and Service cryptanalytic intelligence) in early 1942 enabled Travis, the new chief, to move BP away from Ministry control, and establish direct control of ENIGMA interception. The disastrous war situation at that time forced heavy new commitments to expansion of SIGINT and increase in exploitation resources.

(TSC) In April 1942, the GAF made a wholesale reallocation of frequencies, but callsigns remained predictable. This change was solved by luck and hard work. The Air Section at BP, without access to ENIGMA decrypts, found [redacted]

[redacted] traffic was obtained from Black Market receivers, and the ENIGMA search effort was used to find links passing [redacted] which was generally indistinguishable from ENIGMA traffic. The log readers (people who read radio operators' logs to try to identify the German wireless nets, and understand how the German nets worked) then found [redacted]

[redacted] as a result of circumventing intercept control that had concentrated on exploitable ENIGMA links.

(TSC) By this time, there were expanding parallel traffic analysis efforts in Hut 6, Hut 3, and Beaumanor Army Y station, using different methods and materials. The Log Party began to reconstruct nets from logs and the callsign book, and used ENIGMA traffic, non-ENIGMA traffic, and non-ENIGMA decrypts--contrary to the policy of keeping high- and low-grade SIGINT separate. The Fusion section began to study net content, i.e., what kind of intelligence passed on a net, as well as defining the net structures. Intercept control was vital because of the volume of traffic and shortage of operators, and 3L was established in Hut 3 in September 1942 to inform Intelligence Control of the tasking requirements for intelligence.

(TSC) By December 1942, there were 300 receivers (sets) on ENIGMA, 50 GAF and GA keys, and 1600 deduped messages per day. GAF radio security was generally much inferior to GA radio security. ENIGMA interception was about one quarter of all Y (radio intelligence, except cryptanalysis) interception, and the Army Y stations were the main source.

(TSC) On 1 January 1943, the German Army introduced a new F callsign book, along with some new methods of changing their callsigns. However the new book was [redacted] derived from the E callsign book which had been captured in 1941.

(TSC) The first signs of real crisis came in May 1943, at a time when exploitation and callsign prediction were flourishing. There was a large scale German Army communications exercise in France and the low countries, which produced a large volume of traffic, but none of the keys were readable. Inference from traffic externals was tried for the first time. The real crisis came on the heels of this, when the OVERLORD planners, preparing for the invasion of Normandy, began to demand German Army decrypts. Traffic analysis was asked to steer the intercept system onto GA nets in support of the invasion, and the Air Ministry, which had dominated control of ENIGMA SIGINT, had to yield to the demands of Allied ground forces.

(TSC) The next crisis developed in Autumn 1943. The German Army dropped almost all of its discriminants on 1 September 1943, but the effect was minimized by the ability of the Army Y stations to identify the traffic. Two months later, the Luftwaffe (unforeseen by Hut 6) also dropped its discriminants, causing a catastrophic pileup of traffic, totally unsortable without discriminants, and almost all processing and cryptanalysis was brought to a halt.

(TSC) By good fortune, Hut 6 discovered that one of the analysts in the Quiet Room, who had been solving the discriminant system, had a detailed knowledge of both the radio nets and the GAF order of battle, since he had worked from both logs and decrypts. The Quiet Room and the Y stations managed to solve the crisis, but only after the unsortable traffic had piled up for some weeks. They had to develop completely new methods of sorting the incoming traffic by frequency and callsigns, rather than by the now absent discriminants. Traffic analysis and SIXTA suddenly became indispensable to SIGINT operations.



~~(TSC)~~ By 1944, as invasion preparations advanced, the SIGINT situation was good: both high and low level cryptanalysis had continuity, trained staff and equipment, and were reading currently. The FISH (German Cipher Teleprinter) exploitation was developed as an alternative in case ENIGMA failed. The intercept operations were able to work from predicted callsigns and frequencies. The traffic analysis had almost complete knowledge of German nets, order of battle, procedures, and the callsign books. SIXTA was integrated with cryptanalysis and intelligence analysis. 2000 to 4000 current high level decrypts were being processed daily.

~~(TSC)~~ On 1 April 1944, the Luftwaffe made an expected callsign book change, and Hut 6 made preparations for this which resulted in a complete disaster and a pileup of all incoming traffic. However, the Y stations, who had not been informed or consulted about the change, and therefore had made no advance preparations, nevertheless were able to solve the problem by examining the traffic itself and determine that the change was only partial. After that, SIXTA had to learn to identify traffic without knowing the callsigns. They then began to sort the incoming traffic on callsign serials, rather than by the inaccurate frequency measurements, a practice that should have been started two years earlier. The integrated traffic analysis and cryptanalysis against GAF and GA in Hut 6 then split vertically into separate Army and Luftwaffe efforts--as a result of the different handling required for the GA and GAF traffic. Thus, the irony that the centralized cryptanalytic effort at GC&CS had divided into distinct Army, Navy, and Air Force channels,

because of divergence in the cryptography of the German services--but the vital resources such as BOMBES were still pooled, and even the U.S. Navy BOMBES were used as much on GAF and GA traffic as on Naval tasks.

~~(TSC)~~ On D Day, the huge volume of traffic, caused in part by deliberate cutting of German landlines, threatened to overwhelm the processing. A huge volume of Army traffic was intercepted, but almost none was read. Some Luftwaffe traffic was read. From D Day on, sorting was an analyst's task, and could no longer be done by clerks according to an exact procedure. Masses of traffic were discarded without being identified.

~~(TSC)~~ By Autumn of 1944, German Army traffic almost vanished as the retreating ground forces went onto landline. The German Army, knowing the ENIGMA was being read, introduced stringent radio and cipher security, enforced by OKW and more significantly by RSHA 10, which included the Gestapo. The frequencies were changed every three days and could not be predicted, and encrypted callsigns, now completely unbreakable, were introduced. Although the Hut 6 cryptanalysts were extremely pessimistic about solving the callsign cipher, the W.O.Y.G. (War Office Y Group at Beaumanor) and their outstations solved the traffic identification problem, producing identifications that were 85% correct at the site, while Hut 6 and SIXTA were helpless. The long experience of the Army operators who had copied the same targets for years was crucial in identifying the German Army nets.

~~(TSC)~~ On 1 February 1945, the Luftwaffe went over to the new encrypted callsigns and frequency change system already adopted by the Army, and a complete SIGINT disaster resulted. Unlike the Army Y stations, the RAF Y stations were unfamiliar with the GAF nets. The RAF operators tried to identify the traffic, but were 50% wrong at first, and cryptanalysis came to a halt because of misidentified traffic. The problem was that there were too many cipher messages that might seem to fit with any crib, and no keys could be broken until the nets were at least partly known. The RAF operators improved, and radiofingerprinting (RFP) combined with directionfinding (DF) proved helpful. At this point the low grade decrypts became vital in providing net identifications. The "Duddery" scheme of testing unidentified messages against already solved keys became overloaded and production of decrypts went down to almost nothing. For the first time, decrypts of ENIGMA traffic were passed first to SIXTA, to help traffic

analysis, before they went to the intelligence analysts in Hut 3, for traffic analysis was more important than reporting.

~~(TSC)~~ During 1944, the Germans had tightened lower level hand ciphers so much that [redacted]

[redacted] After [redacted] 1945 crisis, work concentrated on low level systems (aided by captures) and many low level decrypts were reported as intelligence, because of a paucity of current ENIGMA decrypts.

~~(TSC)~~ Fortunately, the FISH and Naval ENIGMA traffic continued to be currently readable, and as the end of the war approached, the RAF radio operators were gradually able to sort and identify the traffic, but the whole problem of traffic analysis was thrown back onto the Y stations--where it had been in 1940.

~~(TSC)~~ The quality of intelligence against the German Army declined with one notable consequence that the American armies invading Germany in April 1945 turned south to attack a nonexistent "Alpine Redoubt." In addition, the traffic that was broken was often weeks old.

~~(TSC)~~ The harsh lesson was that without successful traffic analysis, the rest of the highly leveraged ENIGMA effort, which depended utterly upon good cribs and encipherments across systems, collapsed even though the cribs and reencipherments still occurred, because the unsorted traffic swamped the rest of the analytic process.

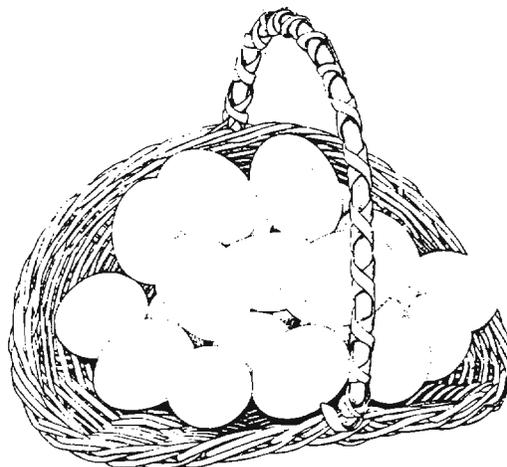
Footnotes

1. British cryptanalysts, and other British personnel at radio stations, London ministries, and elsewhere who were doing parts of what later was recognized as "traffic analysis."
2. Government Code and Cipher School, located at Bletchley Park from 1939; part of GC&CS moved back to London in 1942 for Diplomatic traffic.
3. The section of GC&CS in which decrypts of German Army and Luftwaffe traffic were converted into intelligence and intelligence advisory messages. J.E.S. Cooper, GC&CS Army and Air Force Sigint, XII, 318.
4. The section of GC&CS in which the cryptanalysis and exploitation of the ENIGMA

traffic of German Army and Luftwaffe was carried out; later, traffic analysis was located in the same building and called SIXTA. Cooper, p. 318.

5. In March 1942, a "Quiet Room" was established in the Hut 6 Central Section (which controlled intercept coverage and also identified incoming traffic to research discriminants; an unexpected result of the analysis mode was the discovery that discriminants were derived from a predetermined system. Cooper, pp. 157-8.
6. A Section of GC&CS which kept records of headings and beginnings of all messages, and studied them to see if this would give useful information to other sections. Cooper, p.18.
7. Receivers became available in quantity as a result of U.S. support, and operators in training, using these receivers, were given operational targets to cover as part of training. They were outside the administrative control of 3L, which tasked interception for intelligence, and thus provided a useful surplus capacity, not accounted for, which could be given useful tasks to help Hut 6, without being stopped by 3L. Cooper, pp. 252, 281-2.
8. Each ENIGMA network was allotted a monthly column-allotment "Serial" from the call-sign book, providing a different column of callsigns for use on every day of the month and recurring from month to month; the order in which the 31 columns had been chosen to form this "Serial" was apparently haphazard. Cooper, pp. 52-3.
9. Ober Kommando der Wehrmacht, an organization established by Hitler to control the three Services and coordinate them. It was given central COMSEC authority in 1944.
10. Reich Sicherheit Haupt Ampt = Supreme National Security Board. This organization contained the Gestapo, Security Service (of the SS), Abwehr of OKW and OKW/Chi, the cryptologic agency.

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



IS THERE AN

OLD CROW

IN YOUR FUTURE?(U)

by Ron Cole



P.L. 86-36



In April 1981, the National Office of the Association of Old Crows (AOC) authorized the establishment of a Chapter to be headquartered in the Fort Meade/metropolitan Baltimore area. The Chapter, called the "Chesapeake Bay Roost," is to serve the needs of those in the Maryland area who are interested in the electronic warfare arena. In our first year, the Chapter has grown to the fourth largest in the nation with more than 540 members, more than one-fourth of whom work for the Agency.

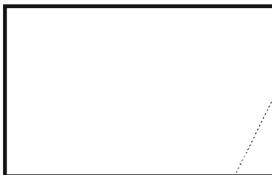
In May 1981, the Director of NSA (an active Chapter member) pointed out that NSA has become a recognized leader in the AOC annual national symposia by providing the electronic warfare community with an appreciation of the SIGINT/COMSEC contributions to solving electronic warfare problems. Agency personnel have presented papers at many of the national symposia; at the symposium last year, [redacted] (W2) was given the award for best presentation.

The AOC is a non-profit professional association of individuals interested in the science of electronic warfare. Its membership includes members of all four services (officer and enlisted), Department of Defense civilians, NATO and other friendly nations' personnel, members of private industry, and members of educational institutions. Membership is open to all grades and ranks, and currently represents a very interesting cross section of society.

The Chesapeake Bay Roost is currently meeting every other month, with luncheons featuring such speakers as General Faurer, General Larson (USAF-ESC), and Admiral Gallotta (USN), and has scheduled General Stubblebine (USA-INSCOM) for its June meeting (23 June, 1100-1300, Ft. Meade Officer Club).

The AOC was organized in 1964 to exchange data on the technical and operational aspects of electronic warfare. The organization has since grown to 58 chapters with more than 32,000 members worldwide. The name "Old Crows" emerged from the first large-scale use of electronic warfare during World War II. The receivers and transmitters used in this effort were produced under the common equipment codeword "Raven." Common jargon later changed the term "Raven" to "Crow" and the group of professionals engaged in electronic warfare became "Old Crows."

If you are interested in joining, the fees are \$15.00 a year (\$7.50 for students), for which you receive a one year subscription to the "Journal of Electronic Defense" (12 issues), an AOC coin, a membership certificate, and a membership card. The following members work within NSA and may be contacted for membership applications:



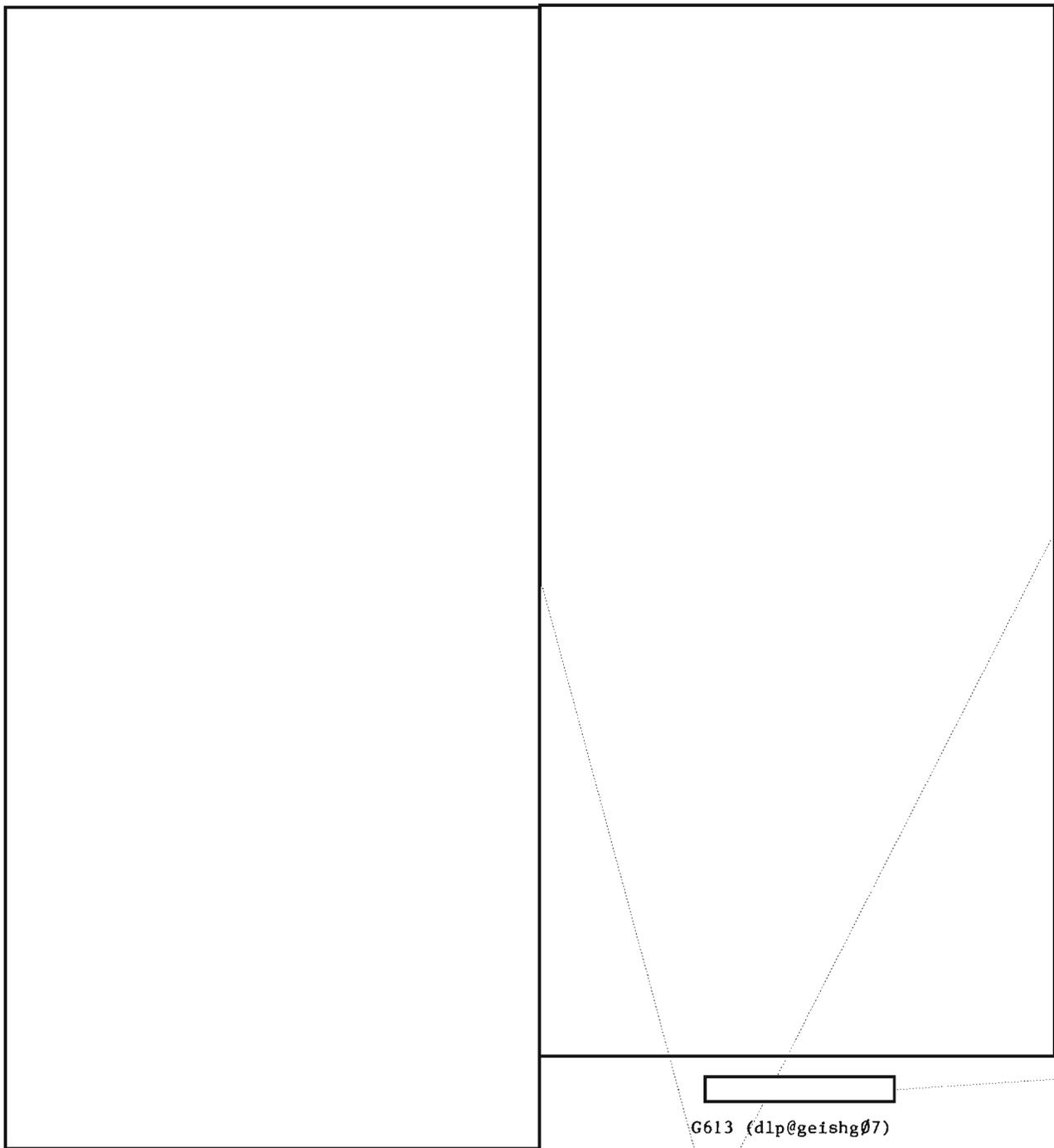
- (President) x8150s
- (Secretary) x8757s
- (Treasurer) x8745s
- (Membership) x8150s
- (Historian) x8893s
- (Programs) x3083s

P.L. 86-36

BUST Answer (c)

by

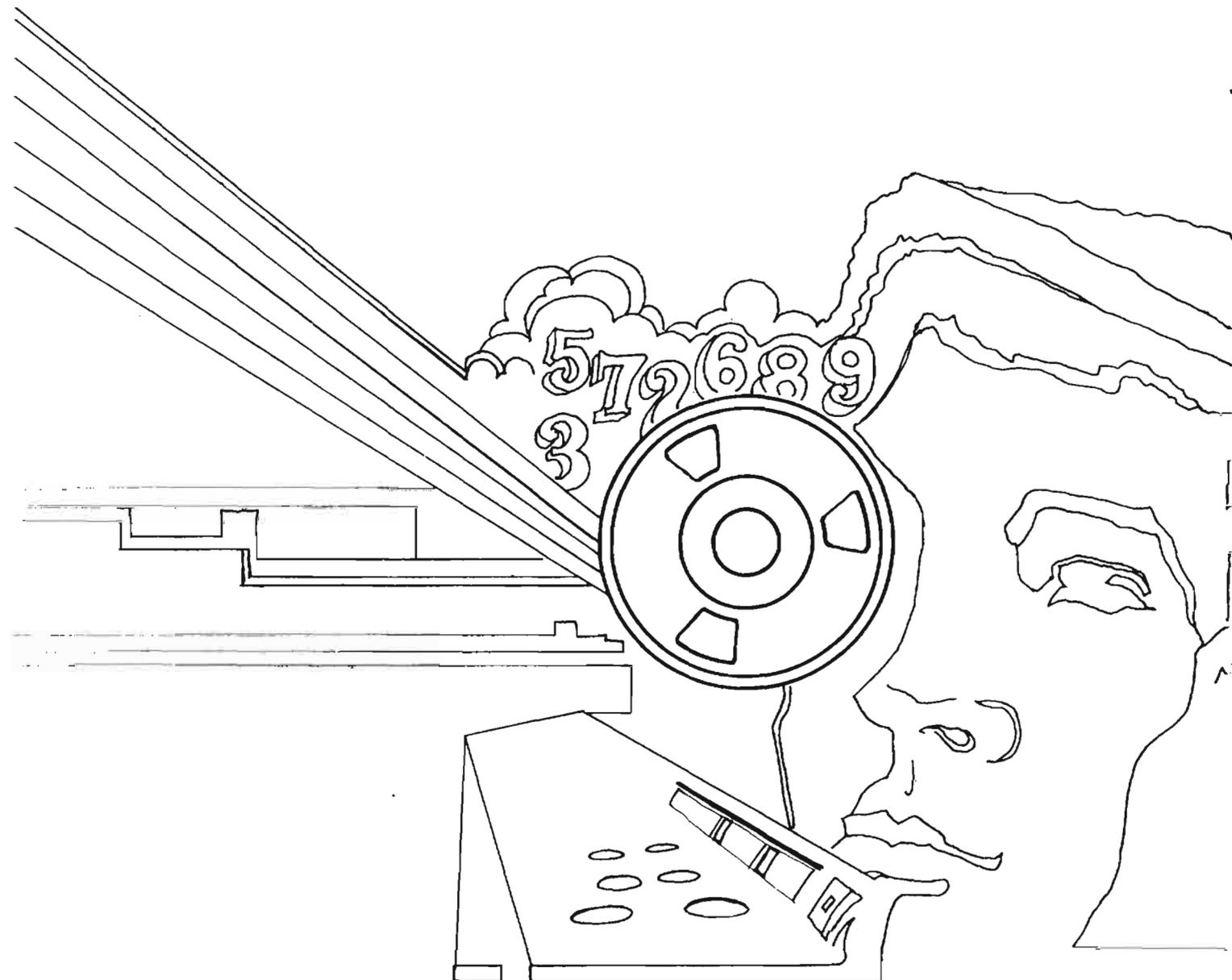
P.L. 86-36



P.L. 86-36

G613 (dlp@geishg07)

~~TOP SECRET~~



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~