DOCID: 4019706

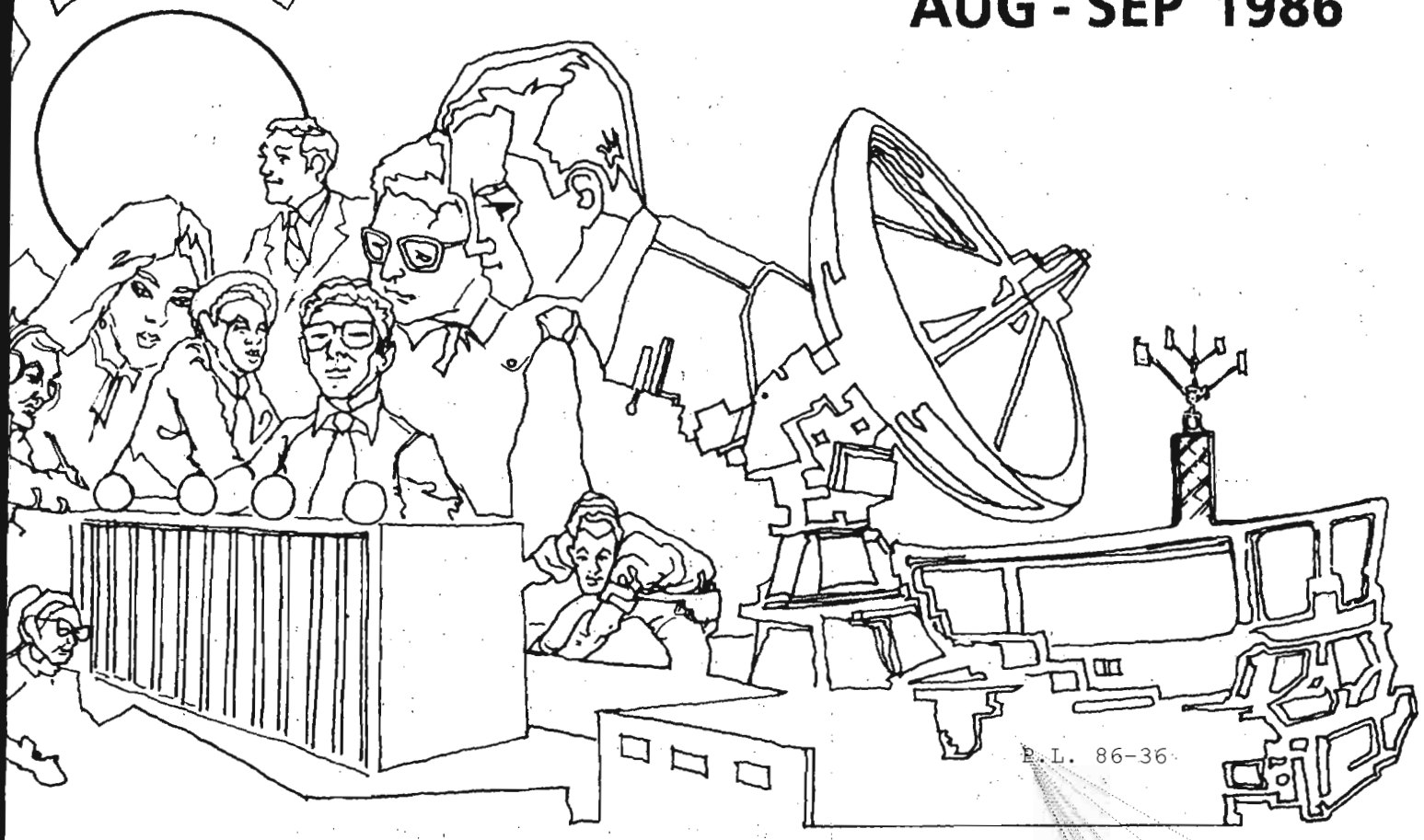
~~SECRET~~

Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54778

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

AUG - SEP 1986



P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

DOCID: 4019706

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XIII, Nos. 8-9 ..... August-September 1986

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Collection ..... (963-5877)
Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-5238)
Cryptolinguistics ..... (963-1596)
Index ..... (963-5292)
Information Security ..... George F. Jelen (963-1211)
Information Science ..... (963-1145)
Intelligence Research ..... (963-5283)
Language ..... (963-3057)
Mathematics ..... (963-5566)
Puzzles ..... (963-6430)
Science and Technology ..... (963-4191)
Special Research ..... Vera R. Filby (968-8014)
Traffic Analysis ..... Robert J. Hanyok (963-5734)

Illustrators ..... (963-3057)
..... (963-6211)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, HQ 8A187

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptolg at bar1c05
(bar-one-c-zero-five)
(note: no 'o' in 'log')

Always include your full name, organization, and secure phone number.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1
Please do not phone.

Contents of CRYPTOLOG should not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

GOOD BUREAUCRATIC WRITING (U)

P.L. 86-36

A contradiction in terms?

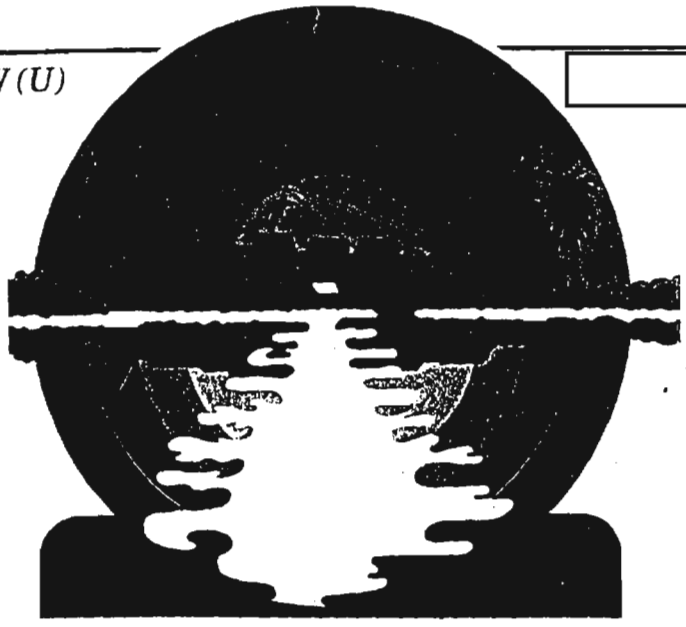
No! It's just that good bureaucratic writing is uncommon. Something strange gets into people when they compose official documents. They forget that the intended readers are the very same human beings they've been communicating with all along.

Maybe all they need is a good example. There's one beginning on page 21. Note that it is short though the information is complete. It can be scanned readily. It reads well. The tone is good. And, marvel of marvels, it states plainly that there is a change of concept, and tells why. Such directness is seldom found. It is efficient as well as refreshing. After all, the population to whom this is addressed is composed of senior professionals in the intelligence business. These people, let us hope, would inevitably find the needle of information in a haystack of gobbledy-gook. It might take them longer, that's all.

Just to show that this example is not unique {single, sole, one-of-a-kind} but merely unusual {rare, exceptional, remarkable}, there's another example beginning on page 6. It's a very readable, nay, fascinating, budget proposal. Surely it moved mountains!

DOCID: 4019706

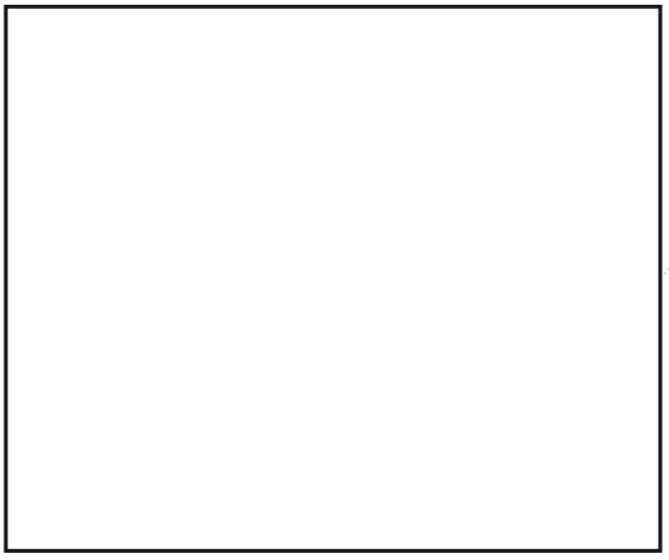
SOMETHING NEW (U)



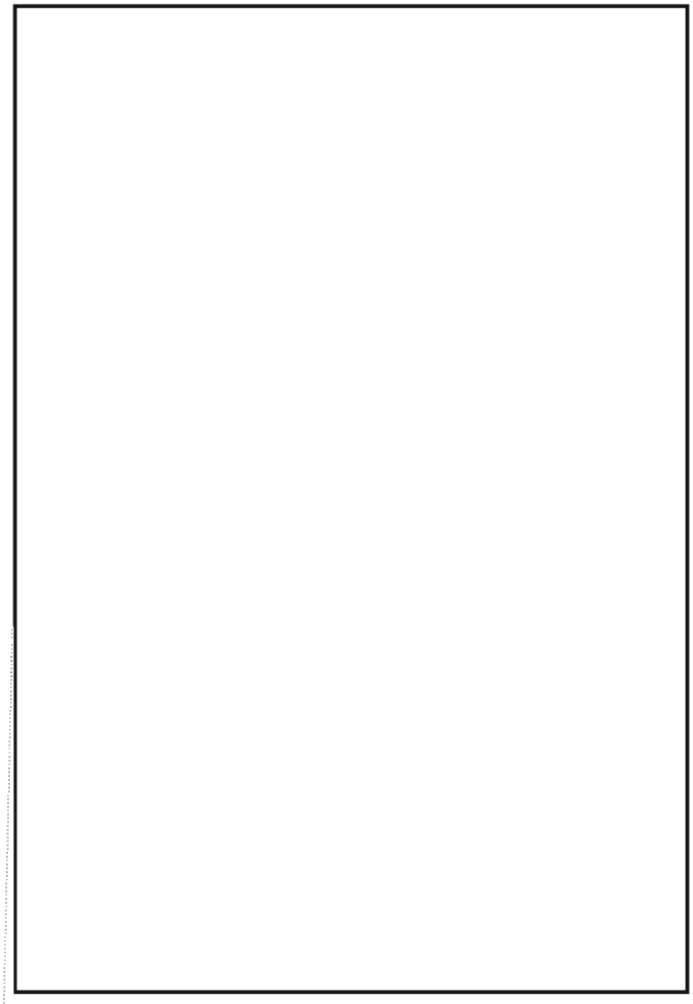
TARGETING NARCOTICS TRAFFICKERS ~~(S-CCO)~~

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

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



AUTHORITY



(U) One principle underlying the ruling is that there is no reasonable expectation of privacy for the radio communications of narcotics traffickers. Therefore, there is no general Fourth Amendment preclusion of USSS interception of such communications and of the monitoring and targeting of US persons who are parties to the radio communications of ships and aircraft involved in narcotics trafficking.

~~(FOUO)~~ Special procedures were approved by the Acting Attorney General in December 1984 which authorize intercept and direction finding against persons whom the USSS reasonably suspects to be engaged in international narcotics trafficking. An international trafficker is defined as any person engaged in buying, selling, manufacturing (from cultivation to refining), or transporting a controlled substance as defined by the Attorney General, where such activities cross international boundaries.

US POLICY

(U) Narcotics were legally imported into the US for more than a hundred years. By the beginning of this century there was strong sentiment to outlaw alcohol but little public concern for the widespread use of narcotics. Drug stores and grocery stores sold narcotics without a prescription and mail order houses distributed them as cures for any number of ailments.

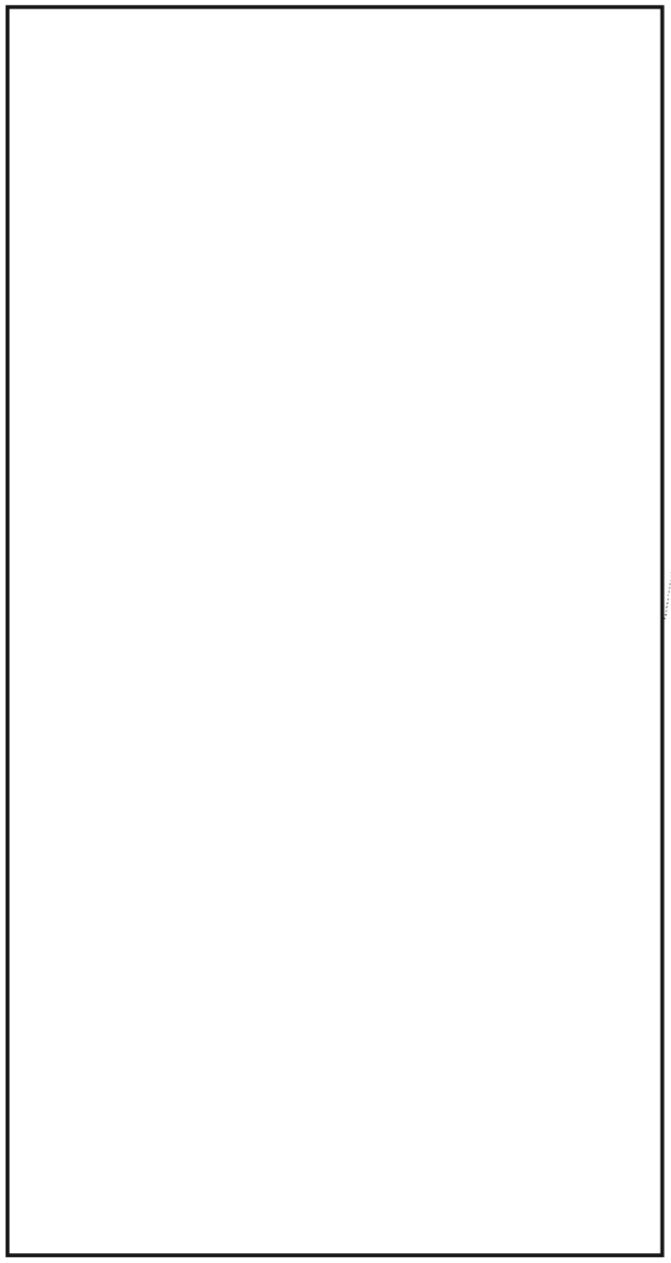
(U) On December 17, 1914, President Wilson signed the Harrison Narcotic Act, establishing the foundations of federal drug law enforcement. Since it was basically a tax on narcotics, Treasury was left to enforce it when it became law on March 1, 1915. The first step in monitoring international commerce in opiates was passed in 1922 and was called The Narcotic Drugs Import and Export Act.

(U) The Federal Bureau of Narcotics was established on July 1, 1930 and in September President Hoover appointed Harry J. Anslinger Commissioner of Narcotics, a position he held for more than three decades. It was Commissioner Anslinger who initiated the enduring US drug policy which maintains that the solution to the drug abuse problem lies

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

DOCID: 4019706

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



with the foreign nations that produce the illicit drugs.

(U) The White House stated in 1982: " . . . the elimination of illegal drugs at or near their foreign source is the most effective means to reduce the domestic supply of these substances." There is evidence that US efforts to control the production of drugs abroad have been largely unsuccessful. Unfortunately, narcotics involves developing nations in debt and in need of US dollars. The producing nations argue that the product would not exist were it not for the demand for the illegal drugs, while Congress accuses the State Department of giving too little high-level attention to the drug problem.

THE NATIONAL BORDER INTERDICTION SYSTEM

(U) In 1982 the National Narcotics Border Interdiction System (NNBIS) was established to combat drug smugglers at the US borders. It collates the intelligence, assesses the threat to the region, prioritizes smuggling targets, identifies resources available to interdict those targets, and recommends actions to the participating agencies. These consist of 14 Federal agencies and 14,000 state and local law enforcement entities that either have a role in drug enforcement or no statutory bar to such a role. The purpose of NNBIS is to increase the various agencies' effectiveness through cooperative and coordinated efforts.

(U) Reservations concerning NNBIS are many. Some suggest that NNBIS isn't needed because organizational coordination is not the problem and that reorganizations serve only to confuse the law enforcement community. State and local law enforcement agencies complain that coordination with NNBIS is virtually nonexistent and that NNBIS has merely confused the national drug enforcement effort and disrupted traditional working relationships with DEA, Customs, and the Coast Guard.

(U) Many people believe that coordination among DEA, Customs, and the Coast Guard is a problem. Note that the US Coast Guard is a part of the Department of Transportation, the US Customs Service is part of the Department of the Treasury, and the Drug Enforcement Administration is part of the Department of Justice. As in any bureaucracy, they sometimes don't talk to one another because of territorial competition. Increasing agency coordination for an effective drug enforcement effort is not yet a reality, and the jury is still out on the effectiveness of NNBIS as the answer.

NARCOTICS INTELLIGENCE GATHERING

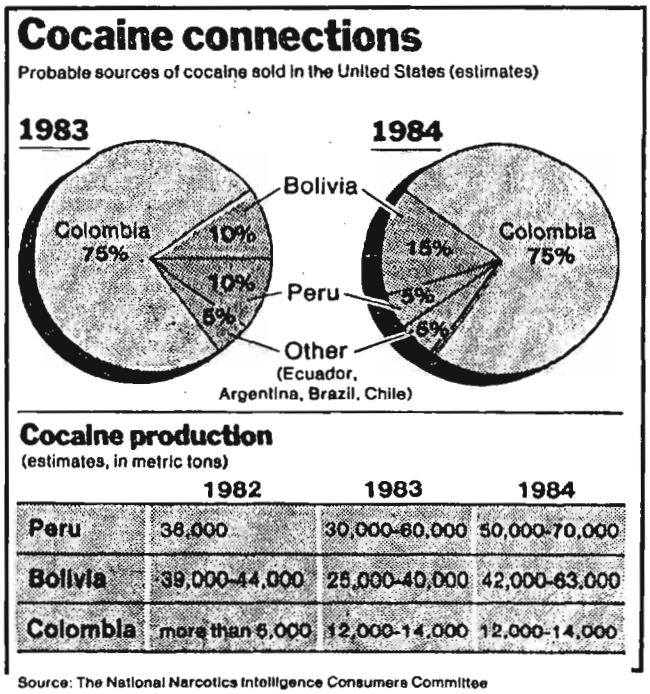
(U) DEA, created in July 1973, is the lead Federal agency in enforcing controlled substances laws and regulations. Its primary responsibilities are to: investigate major narcotic violators; enforce regulations governing the legal manufacture, distribution, and dispensing of controlled substances; manage a national narcotics intelligence system; coordinate with federal, state and local law enforcement authorities and cooperate with counterpart agencies abroad; train and conduct scientific research; and exchange information in support of drug traffic prevention and control.

(U) The El Paso Intelligence Center (EPIC) is an interagency operation managed by DEA with participation by nine other federal agencies and working agreements with 45 states. EPIC provides a nationwide intelligence clearinghouse for drug enforcement information. Most information produced by EPIC is marked "DEA SENSITIVE" because it does not qualify for classification as National Security Information. SIGINT received by EPIC pertains to narcotics information only and is used to corroborate other sources. Fewer than six persons with special intelligence clearances have access to SIGINT, and they are forbidden to remove, sanitize, or enter it into other databases.

STATUS

[redacted]

(U) Interdiction, however, is difficult. Most marijuana is smuggled into the US by ship and most cocaine by aircraft. Since cocaine is easier to ship and the profits are greater for dealers, there has been a predictable switch to cocaine. Ironically, the success of the US effort against marijuana has had the effect of weaning the



Cocaine production
(estimates, in metric tons)

	1982	1983	1984
Peru	36,000	30,000-60,000	50,000-70,000
Bolivia	39,000-44,000	25,000-40,000	42,000-63,000
Colombia	more than 6,000	12,000-14,000	12,000-14,000

Source: The National Narcotics Intelligence Consumers Committee

American public off marijuana and onto cocaine. The children who once smoked marijuana may now be smoking crack.

~~(SC)~~ NSA is only one of many players who deal with the international narcotics problem, but our input, modest though it is, is invaluable. SIGINT contributes to national estimates forecasts and to studies on the narcotics problem, and often gives US policy makers an indication of how effectively foreign aid earmarked for narcotics eradication is being used.

[redacted]

~~(S)~~ In April 1986 President Reagan signed the National Security Decision Directive that "will permit the armed forces to dedicate personnel and equipment ... to fight drug trafficking. Now the armed forces will be able to help in almost any area of drug law enforcement except arrests, seizure of materials and apprehension of suspects, as long as their primary defense mission is not jeopardized." Drug trafficking in the US Southern Command is seen as feeding arms supply and insurgency which destabilize Latin America. In this light, the new military role in the drug fight becomes more

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

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

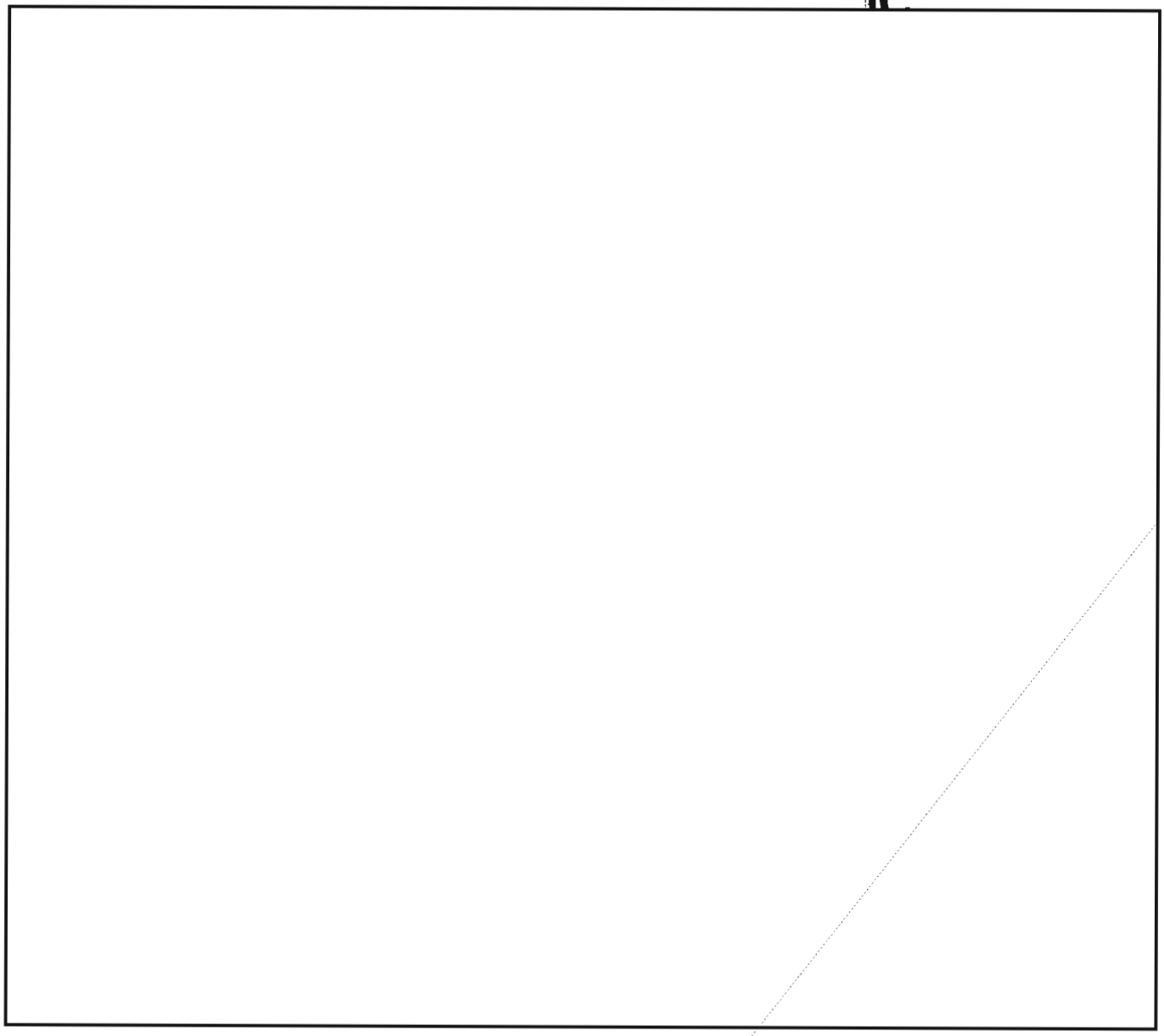
DOCID: 4019706

understandable. Defense Secretary Weinberger, however, once termed the idea "very dangerous and undesirable." Civil liberties advocates fear covert surveillance of US citizens, preferring that President Reagan ask Congress to fund the regular agencies.

~~(S-CCO)~~ But while the Defense Department budgets have soared in the last five years and DoD has been given an increased role in combating narcotics, Coast Guard ships sometimes remain in port because of the lack of gas and manpower to interdict drug smugglers. Priorities need to be adjusted so that enforcement agencies can act upon SIGINT when it is applicable. Moreover, it is clear that the federal law enforcement community needs better organization and coordination on narcotics interdiction strategy. It may also need to better define the role SIGINT can play in this overall strategy. □

Editor Note:

Readers might be interested in comparing present efforts to combat narcotics trafficking with similar efforts to interdict rum runners during Prohibition, as described in the memo beginning on the next page.



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

DOCID: 4019706

Rum Runners, 1930 (u)

DATE: 10 October 1930

MEMORANDUM FOR THE COMMANDANT

SUBJECT: Radio Intelligence; Establishment of Cryptanalytic Section at Headquarters and Intercept Stations in the Field

In accordance with your instructions of 3 October, I took up with Customs the matter of holding in abeyance the transfer of Mrs. Friedman, cryptanalyst, and her assistant, from the Coast Guard Intelligence Office to the Divison of Special Agents, Bureau of Customs, pending the determination of the question as to whether or not the Coast Guard could undertake the establishment of a cryptanalytic section at Headquarters as a basis for a radio intelligence service in the field which would put the enforcement agencies (Coast Guard, Customs and Justice) in immediate possession of specific knowledge of the operations of the smugglers upon which definite action, resulting in seizures and the prevention of smuggling, can be taken.

Customs readily assented to the retention of Mrs. Friedman and her assistant pending developments and, moreover, agreed that the Coast Guard was the logical government agency to handle the radio problem. When my plan was outlined, the Commissioner of Customs, Captain Eble, not only agreed to the Coast Guard undertaking the project but offered to go to Mr. Mills in support of it.

In order that you may be fully acquainted with the problem and its solution a brief summary of the radio activities of the smugglers and the attempts, to date, of the enforcement agencies to combat it is necessary. Practically all operations of the smugglers from the sea are now directed by radio in code and cipher. Without radio the smugglers would be so greatly handicapped that I have no hesitancy in saying that once the Government can gain the upper hand in the control of their radio activities smuggling from the high seas will be reduced 50 per cent. On the east coast there are forty-five radio stations, between Maine and Florida, directing the movements and operations of smuggling craft. There are fifty-eight smuggling craft known to be using radio. The Coast Guard has a record of eighty-one stations in a single group whose operations are directed from the New York area. On the west coast, all smuggling operations on the coast of California are directed by radio from Vancouver and a station on the California coast. In short, communication between ships and shore is essential to the operations of the smugglers on the present organized scale. It is carried on constantly in code and cipher. It is now being intercepted by the Coast Guard and by Customs Agency intercept stations. This intercepted material contains much of the information that the investigative agencies of the Customs and Justice are after the practically all of the plans, including contact points, to obtain which the Coast Guard vessels cruise endlessly.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

About three years ago the late Captain Root took up the matter with Prohibition, and, with the Prohibition Bureau furnishing personnel and the Coast Guard the equipment, intercept stations were established in San Francisco and Florida, and Mrs.Friedman, cryptanalyst, was employed by Prohibition and established in the Coast Guard Intelligence Office to decipher and decode the material. The information thus obtained was most valuable to the Customs Agency and Coast Guard in giving into the hands of the enforcement agencies complete information of the plans and methods of operation of the smuggling rings as well as the personnel engaged in the traffic ashore. With this limited organization valuable information for use in combating the rum-runners was obtained. The uses to which this information was put, and numerous concrete examples of the practical value of this work in the prevention of smuggling can be given from the files of this office.

Up to recently this work was mostly informative but the success obtained with this modest beginning led to an experiment with a 75-foot patrol boat (the CG-210) which was turned over to the Intelligence Office to operate. It was equipped with high-frequency receivers and radio-compass and assigned to duty in the New York Area to:

(1) Intercept and send in for solution the radio communication between rum ships and radio ashore.

(2) Locate and raid illegal radio stations from which the operations of the rum ships are directed.

This patrol boat; under the command of Lieutenant Meals, has done all that was expected of it. Its success in intercepting by high-frequency receivers of the rum-ship operating orders and in locating the illegal stations on shore with its recently developed high-frequency radio direction finders, led to the final step in the establishment of a complete field radio intelligence unit. Through the cooperation of the War Department, Major Friedman, Chief of Signal Intelligence Division, and an expert cryptanalyst, was detailed to the CG-210 for a period of two weeks. We thus had on a single 75-foot patrol boat:

(1) A battery of high-frequency receivers with radiomen to intercept the coded operating orders of the rum-runners.

(2) A cryptanalyst to reduce the intercepted message to plain text.

(3) Radio-compasses to locate the illegal stations.

(4) A Coast Guard officer thoroughly familiar with the operations of the enforcement agencies to immediately act on the information derived.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

In a period of two weeks the following was accomplished by the CG-210:

(1) The code was used by a group of smugglers operating off New York was broken and the operating orders to the rum ships were read as soon as received.

(2) The code was compiled and made available for use by the Coast Guard units.

(3) Two radio stations, one situated in new Bedford, Mass., and one in Coney Island, were located, raided and put out of business. (Coast Guard working in conjunction with Department of Justice agents and Department of Commerce inspectors).

(4) Evidence linking up the NOVA V, recently seized by the Coast Guard, with the radio station was obtained with is deemed ample to indict on conspiracy charges.

As a result of the interception and solution of the smugglers code and the raiding of the station, the operations of the group of rum ships was completely stopped for several days, no contacts were made and the resulting confusion to this group of rum ships was more than all the efforts of the destroyer force and other units combined have been able to effect in months--and it should be remembered that this was accomplished by a single patrol boat with nine men aboard which never went near "rum row." As a result of this two-weeks experiment we have arrived at the point where it has been demonstrated that the radio intelligence unit has passed from the purely informative stage to one of practical application as an invaluable aid to the patrol forces engaged in the prevention of smuggling.

The problem of the use of radio by rum-runners has grown to such proportions during the past year that it has attracted the attention of other government departments, with the result that a recent inter-departmental committee from Justice, Commerce and Treasury was appointed to suggest a solution. The report of the Committee is appended and it will be noted that the conclusions and recommendations show that the problem and its solution is entirely Coast Guard work. In fact, there was no necessity for putting it up to an inter-departmental commitee as the Coast Guard not only has been aware of the situation for years but has had all the elements for its solution at its disposal. It is logically a Coast Guard activity.

Now the keystone of the whole system is the reduction of the rum-runners' codes and ciphers to plain text--the cryptanalyst section--and it is essential that there be established at Headquarters a section in the Intelligence Office capable of breaking the codes and ciphers and supplying the rum-runners' codes and ciphers to the field; and of training the men in charge of intercept stations in this line of work. The set-

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

up required and the cost is appended. Discussion of this will be given in person, as it is quite involved and extended.

It might be well, here, to give a brief summary of the present rum-running situation. In the past year there has been an increase of 34 per cent in foreign rum-runners. We are now back to where we were three years ago with this vast difference, the rum-runners are organized on a basis that makes the methods used three years ago practically obsolete. And their radio communication system is the key to this organization. The actual figures are:

1927	138
1928	109
1929	103
1930	138

One rum-running syndicate pays the man in charge of its radio installations $10,000 a year. The radio communications on the west coast are directed from Vancouver by a radio schoolmaster versed in the most intricate system of codes and ciphers. Rum ships are in charge of former British Naval Officers. Under present conditions on the west coast the Coast Guard is practically impotent. On the east coast the Coast Guard harasses and annoys the rum ships, but the results in proportion to the effort expended is pitifully small. One of the purposes of the radio intelligence unit is to obtain greater results from the same expenditure of effort; in other words, to employ the present equipment of the Coast Guard to the best advantage. The cost of the entire radio intelligence unit is less than the cost of operation of a single destroyer or cutter or of three or four patrol boats, and the results that should be obtained are worth more than the results of operating a squadron of destroyers or patrol vessels.

It must be understood that this subject of radio intelligence is not theoretical nor anything new. The following has been actually accomplished:

(1) Cipher message intercepted and solved showing contact point where and when shore boat is to take load from rum runner. Information given to patrol force, British and American rum-runners seized. (Case ISABEL H--Destroyer Force).

(2) Radio stations on shore directing rum-ships operations and contacts located and raided. (New York area).

(3) Codes and ciphers broken and furnished to field so that operations of rum ships made available immediately to patrol forces. (West coast, Gulf and New York areas).

(4) Evidence obtained by breaking ciphers and codes to obtain convictions on seizures. (Gulf and New York areas--NOVA V).

~~FOR OFFICIAL USE ONLY~~

(5) Information furnished Customs and Justice agents to build up cases of the rum rings ashore which are operating the rum boats.

Concrete cases can be supplied from the files of this office. A development now in process is the location of the rum ships at sea by radio-compass instead of by the cruising of destroyers and patrol boats over thousands of square miles of sea.

The necessary field units can be supplied by the Coast Guard from present equipment and personnel--if necessary taking them from units now producing no results. What must be supplied is the Headquarters' Civil Service unit, costing approximately $12,000 a year.

Now for the other side of the picture. If this organization is not adopted by the Coast Guard, Mrs. Friedman goes back to Customs and works on the intercepts from the two Customs stations. The Coast Guard with its destroyers and patrol on a military basis will continue to patrol the seas and operate precisely as if radio had never been heard of, spending hundreds of thousands of dollars in an effort to stumble across. the information that is constantly on the air, i.e., the location and contact points of the rum-runners. Any one familiar with the history of the British Navy in the World War could hardly fail to appreciate the value of this work.

The personnel in the field are interested in this phase of operations and are wondering why Headquarters hasn't long ago developed an organization along these lines. Radiomen construct short-wave receivers, get the traffic and send it in to Headquarters--and there the matter ends. There is decidedly a question of morale involved. There is no brooking the fact that there is now spreading in the Service a sense of futility of effort; and from that a feeling that a demonstration is all that is required; and it is a very short step from that to the belief that a demonstration, rather than actual result is desired by Washington. The cost of this radio intelligence unit is so small in comparison with any other unit as to be insignificant, and it cannot fail to justify this expenditure.

It is therefore recommended:

1. That the Commandant go to Mr. Mills (or to Governor Lowman first and then to Mr. Mills) to get authorization for $14,660 to establish the central cryptographic section at Coast Guard Headquarters (civil service). It would appear that the best procedure is to request that it be authorized for the C.G. appropriation 1930-1931 available 1 July, 1931, and if necessary take this amount from various other items so that the total of the appropriation will not be increased. I deem this matter of sufficient importance to justify asking for a deficiency appropriation to cover but in view of the present fiscal situation, doubt if it

~~FOR OFFICIAL USE ONLY~~

could be obtained regardless of the merits and urgency of the proposition.

2. That three 75 foot patrol boats be turned over to the Intelligence Unit to be equipped and manned similar to the C.G. 210, each boat to have the following personnel:

1 Commissioned officer in command
1 C. B. M.
1 B. M. 1/c
1 C. Mo. M.M
1 M. M. M. 1/c
4 Radio Men 1/c
1 S.C. 1st class

3. That the following personnel be assigned to the New York Intelligence Unit under Lieutenant Meals:

1 Commissioned Officer
1 Yeoman
1 Radioman (Chief or 1st Class)
6 Radiomen 1st class
6 Carefully selected Warrant officers for preliminary training under Meals to be brought to Washington for training under cryptanalytic section when latter is established.

4. It is realized that the personnel asked for above are not available but the importance of this organization justifies, if it does not make mandatory, the withdrawal of the personnel required from other units, particularly non-producing units. The personnel of a 75-footer as now authorized will supply the personnel of each 75-footer assigned to this work.

5. It is realized that the commissioned officers required are not immediately available, and if it is not desired to take them from other units - and I would not hesitate a minute to put a destroyer or other unit out of commission to supply them for this work - carefully selected warrant officers can be substituted to command the 75-footers until commissioned officers are available.

As stated above the Commissioner of Customs, Captain Eble, deems this the most important development to combat smuggling that has arisen and is 100 percent behind the Coast Guard in this plan and will go to Governor Lowman and Mr. Mills in support of it. The inter-departmental situation makes immediate action necessary on the part of the Coast Guard. (This will be explained in person.)

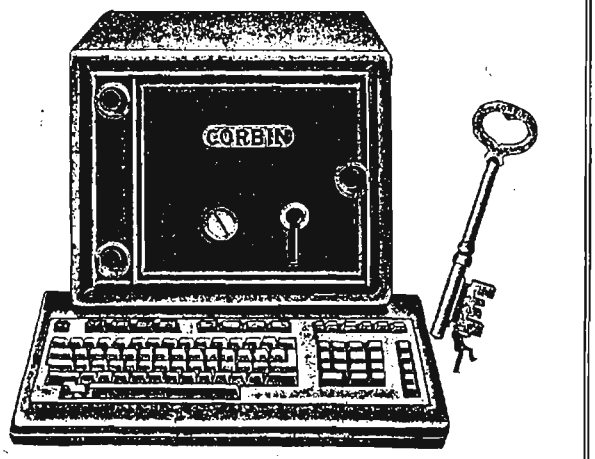
F. J. GORMAN

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

Editor's note:

Computer Security is in the air. In the same week we received an article, a Letter to the Editor, and a book review on the subject, printed below, as well as an item for the Bulletin Board.



Enter Your Passphrase, Please (U)

P.L. 86-36

C11

This article is classified ~~FOR OFFICIAL USE ONLY~~ in its entirety.

In fulfillment of NSA's expanded responsibility in the field of computer security (COMPUSEC), a major effort has recently been undertaken to support enhanced password security at the Agency. Soon users of CANDE and SOLIS will be introduced to the results of this effort. This article will give you an idea of what the new system will be like as well as the history and rationale behind this change.

In an attempt to provide enhanced security, better guidance, and rationale for the use of passwords on a computer system, the National Computer Security Center (NCSC) published the *DoD Password Management Guideline* in April 1985. The document is based on the best security practices on existing computer systems. The underlying principle of a secure password system is that the passwords are kept secret at all times. The major features advocated in this guide-line are:

- that users should be able to change their own passwords;
- that passwords should be machine-generated rather than user-created; and
- that certain audit reports (e.g. date and time of last login) should be provided by the system directly to the user.

The Guideline explains what a good password management system should be able to do, and outlines the responsibilities of users and system security officers in the secure use of passwords. It recommends and suggests alternatives for setting up a password management system, and explains how to calculate such things as the maximum password lifetime, password space (the maximum number of valid passwords that can be generated by the system), and the probability of someone guessing the password for a given password space and lifetime.

When users change their own passwords, no one but the user is involved in that change, and the user is supposed to be the only person who knows the password. But many users lack imagination and select passwords that are easy to remember, resulting in passwords that can easily be associated with themselves. This makes guessing passwords fun and rewarding for anyone trying to gain access to someone else's account.

Machine-generation takes the guess work out of selecting secure passwords, but results in passwords that people dislike because they are

DOCID: 4019706

usually too hard to remember, so they jot down such passwords and leave them by the terminal for handy reference -- by both the authorized user and unauthorized "hacker" alike. Even systems that attempt to provide pronounceable machine-generated passwords often fail to provide a certain linguistic reality which most people need to help remember them. However, there is a way to generate passwords that are both secure and that have linguistic properties that make them much easier to remember. This is using machine-generated passphrases, consisting of a combination of real words, with or without semantic meaning.

To demonstrate the utility of its guideline and the practicality of machine-generated passphrases, the Division of Standards at the NCSC embarked on a project to implement its *DoD Password Management Guideline* on one of the existing computer systems at the National Security Agency. For the experiment, the computer system selected had to be one that would significantly benefit from the implementation, one on which people could really see the tenets of the Guideline in action, and one that could readily use machine-generated passphrases. As the first step they examined the computer systems at NSA and had discussions with system security officers, computer system personnel, and users. Finally, they selected the WINDMILL / PULPWOOD Burroughs system, and began work in May 1985. . The completed Passphrase Management System will appear first on CANDE, followed by implementation on SOLIS.

Under the current system, users are sent a machine-generated, eight-character random alphanumeric password every six months through the mail. The user receives a punched card containing the password and a numbered information form and receipt to be filled out and returned to the Tech Support office acknowledging receipt of the password and that user's continued use of the system. The number on this form matches an identical password card that is filed in the Tech Support office for use whenever a user forgets the password and cannot find the card.

At an appointed time, most often over a weekend, all passwords on the system are changed. As you might guess, the next work day there are a lot of locked terminals as users forget to use their new passwords or have trouble entering them. (Three bad logins locks a terminal.) Paradoxically, the strongest point of the machine-generated password has proven to be its weakness: because random-generated passwords are so difficult to memorize, many users keep their new password on a card near their terminal for easy reference.

Under the new Passphrase Management System, three words are randomly selected from a data base of three to six letter English words and displayed on the user's terminal. The user may use those three words in any desired order to make up a new passphrase. If the set of words proffered does not yield a readily remembered phrase, the user may request another set, up to a maximum of ten sets. Once the word order has been selected, the user must enter the new passphrase correctly twice in succession to verify that it has been entered correctly and to reenforce the new passphrase in the user's memory. If a new passphrase has not been successfully selected within ten tries, the user will be locked out of the system and advised to contact the system security officer for assistance.

A new passphrase is good for a maximum of three months but can be changed at any time before then. The system will automatically alert users when their passphrase is within two

~~FOR OFFICIAL USE ONLY~~

weeks of expiration. Users on interactive terminals may change their passphrase at any time in that period. Should the passphrase not be changed by its expiration date, that user's account will be flagged as having an expired passphrase. Once the passphrase expires, the system will automatically invoke the change passphrase routine whenever a login is attempted and will not allow the user to login until a new passphrase has been selected. If the user does not change the passphrase within two weeks after expiration, the account will be locked, and the user will have to contact the system security officer to get back on the system.

To log in using this new passphrase system, the user first enters his or her standard userid. The user will then be prompted to enter a chargecode, consisting of a classification level, a function code, and a job number. Next, the user will be prompted to enter the passphrase, which wherever possible will be concealed. Upon entry of the passphrase, the screen will be automatically cleared. If all the elements supplied are correct, the user will be logged in and given the date, time, and place of both the last successful login and the last unsuccessful login attempt plus the total number of unsuccessful login attempts since the last valid login. This information can alert the user to any attempted penetration of the system using his or her userid. The new successful login data will be stored, the failed login counter cleared and the user given access to the computer. Should any of the information supplied be incorrect, the user will be told that the login was invalid and a record will be made of this incorrect login by incrementing the failed login counter and storing the date, time and terminal identification.

The user will be allowed a total of ten consecutive unsuccessful login attempts before the account is locked and the user required to contact the system security officer before again being given access to the system.

It is considered a security violation for more than one person to know the password or passphrase for any given individual userid. Thus this system will not allow more than one user to be logged in under a given user account. Special groupids may be established for those projects where more than one user needs to share access to the same computer resources. A user may be a member of as many as five groups, and a group may have as many as thirty members. At login time, the user will enter his or her own individual userid, then a comma, followed by the groupid. When prompted for the passphrase, the user will enter his or her personal passphrase. The userid and passphrase will then be authenticated, and if correct, group membership and classification level will be checked. If everything is correct, the user will be logged in under that groupid. Any problems will result in an unsuccessful login attempt for that user.

Users of the Burroughs system have always included a classification level within the chargecode as part of the login sequence. In the past, the system checked only to see if the classification given was at a meaningful level. Under this passphrase management system, the classification level is also checked against the user's own security profile. For example, if the user has a maximum clearance level of SECRET and tries to login at TOP SECRET, the login will be unsuccessful. Or should the user try to login at UNCLASSIFIED when that particular user's account has CONFIDENTIAL as a minimum access level, the system will also deny access. While the latter illustration may seem an unnecessary precaution, it is a measure to

DOCID: 4019706

protect extremely sensitive data from accidentally finding its way into an unclassified file. A user may also change the chargecode during a given session, but again, the user must specify a level for which he or she has access privileges or the requested change will not be accepted.

A record is made of every action processed by this new system. This information is stored in special audit files for use by the system security officer. There is a general audit file containing all the actions processed by this system, and in addition, another special audit file that contains a subset of those actions that could be indicative of a security problem. Some of this information is also given directly to users at login time in order to help users detect problems with their own accounts. However, the system security officer has these more comprehensive files available for detecting patterns of behavior which could signal overall security problems.

The Passphrase Management System has undergone extensive testing and evaluation and should be fully operational on CANDE by the summer of 1986. This project has shown that the principles propounded in the *DoD Password Management Guideline* can be effectively implemented. The recommendations and specifications in the guideline can be tailored to meet the security needs of any computer system. Keep in mind that while most of the features in the guideline can be automated, much of the effectiveness of any system will depend on the users working with the system security officers to understand and follow good password management practices. □

To the Editor:

In regard to the article "User-Friendly Passwords" in the May-Jul 86 issue, I find a problem with the premise stated in the first part of paragraph three: "the need to generate ... passwords" implying that password generation is a user responsibility. I agree with the DoD Computer Security Center's position, "Passwords should be machine-generated rather than user-created." People are far too predictable when picking passwords. Knowing something about the person allows an attacker to vastly reduce the number of possibilities in attempting to guess passwords. Machine-generated passwords (or pass phrases) are much better at assuring that passwords are distributed over a large space.

I claim that it is the computer system administrator's responsibility to provide password generators which give the user a fighting chance of remembering passwords that are generated. I claim that passwords that are pronounceable strings like "SEN-SLES-GAR-BYG" are not that hard to remember. Maybe not fun to remember, but not hard. Giving the user some choice in the matter can make the procedure

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

more user-friendly. Some of the author's mnemonic devices could be used to remember nearly any random string if the user is clever enough.

I believe that the author has a valid complaint about how machine-generated passwords are administered on some systems. His complaints about the way LUDLOW is used are understandable. Better human engineering of password generators would be welcome. More information on guidelines for passwords is available in the Center's publication on password management, available from C4.

If one accepts the premise that password generation is a user responsibility, then this article has practical suggestions on how users can do a better job at meeting the responsibility. But I would challenge the author to come up with a better password generator which meets the Center's guidelines. The basic requirements are not hard to state and they allow for a wide range of creative solutions. Human engineering is important and the author has practical experience in using passwords. Since password generator programs are rarely exercised during the course of a day, they can be large, and very user-friendly.

[redacted] *C51*

P.L. 86-36

OUT OF THE INNER CIRCLE;
A Hacker's Guide to Computer Security
by Bill Landreth. Microsoft Press,
Bellevue Washington, 1985

Reviewed by: [redacted] *C212*
P.L. 86-36

This book is an excellent non-technical introduction to computer security for the lay person. In the first chapter the author describes a hypothetical attack on a corporate computer: a battle of wits between the hackers (who choose the time and place of their attack) and the operators (who wait, detect, and respond). The remaining chapters present a brief history of computers, a history of hacking, and an overview of computer security measures designed to limit hacking damage. These chapters are well organized and the material is clearly explained, so that even non-technical readers will be able to understand it easily. The book closes with an epilogue detailing Landreth's arrest and trial and an appendix giving his evaluation of some commercial computer security devices. I have some reservations about his evaluations, detailed below.

Landreth writes about computer security from personal experience as a hacker; his hobby was breaking into other people's computers. (That's not the only meaning of "hacker," and some people object to it, but Landreth used it and so

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

will I.) He started with a TRS-80 and an Apple II. It was with his Apple II that he discovered the challenge of understanding and controlling other computers through his own; this challenge appears to be the motive force for most of the incidents recounted in the book. Landreth describes how his increasing ability and reputation finally brought him into the "Inner Circle," an informal group of expert hackers who "met" electronically by leaving messages on the computers they had penetrated. It was their superior skill that finally ended Landreth's hacking career; they had penetrated some computers so regularly that they were discovered, traced, and arrested.

Landreth's hacking experience gives the book both its strength and its weakness. His knowledge and interest are reflected in the book's convincing detail, but they affect his objectivity. Successful hacking means using the computer in an unauthorized or abnormal way. (It isn't hacking if they let you in!) Most hackers learn a system's weaknesses by trial and error, usually by exploiting "bad" commands in the programming (those not intended or anticipated by the computer's designer). Landreth implies that few hackers intend harm and that most are harmless. I disagree. Unauthorized entry may destroy data or slow down the computer so much that real work can't get done. Hacking, therefore, is not a harmless pastime.

Another limitation of Landreth's personal approach is his lack of knowledge about the special problems inherent in military systems, such as susceptiblity to espionage. The anti-hacker standards set by Landreth are inadequate to protect sensitive information against professional espionage. Appropriate standards for "Trusted Systems" are described in the "Orange Book," the National Computer Security Center Trusted Computer System Evaluation Criteria. None of the systems penetrated by the Inner Circle meet the requirements even for C1, the lowest level of trust. Landreth also neglects the special problems of embedded computers in modern weapons systems.

Neither omission is a serious flaw in an introduction intended for the general public. But people facing professional espionage or managing embedded computers need more than this book; they need professional defense. □

EXTENDED HOURS

for

LEARNING CENTER #1 (U)

[ ] *E22*

Learning Center #1 (room 2C166, Operations Building #1) is operating on extended hours. The center is open Monday through Thursday, 0700 - 2200. Yes, that's 10 pm!

At the Center there are courses on cryptanalysis and other Sigint disciplines, computers, management, personal development, target studies, office skills, and other subjects. Many are overviews without exams, a good way to try something new.

A list of courses is published quarterly. For more information stop by or call 963-5899 (s) or 688-7922 (b).

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

COLLECTION MANAGEMENT

I PAST,

II PRESENT, *and*

III UNCERTAIN FUTURE (U)

[redacted] G53 P.L. 86-36

~~*This article is classified CONFIDENTIAL CCO in its entirety*~~

Am I a fireman on a diesel-driven collection system?

Am I a relic of the past without a future?

It's time for me to find a psychoanalyst to gain an understanding of my original Agency occupational specialty. For some years now, I've asked myself the following questions: "What is collection management, and why do we need collection managers in NSA?"

These questions are disturbing only because I am certified in this career field and without it I would be qualified only for staff and management positions. I want to believe, therefore, that a need exists for collection managers like me and that the Agency really depends on our work. This is where my schizophrenic problem begins; I want to believe in the need for collection managers, and at the same time, I can't find a real reason for us to exist, at least under our present job description.

In order to understand my problem, you must have at least a basic knowledge about why collection managers were first introduced into the Agency work force. My knowledge along this line is somewhat limited in that collection managers were already on the scene at NSA when I started in 1959. I understand from some old-timers who worked here before me that there were elements in the Agency named GENS (now A Group), ALLO (now G Group), ACOM (now B Group), COLL or COSA (now P5 and a little bit of every other office involved with collection activities), and still others. At that time, there was no Combined Cryptologic Program (CCP) and nearly every element within the Production organization operated as an independent agency.

You must also remember that the signal environment at that time was simple (Morse, voice, and some printer ... which by the way was considered to be an advanced signal type at that time). I can remember statements being made upon my arrival at NSA that Morse was on its way out and printer was going to be the way of the future and, by the way, how would we be able to cope with such technology?

Because there were so few types of signals available for NSA to exploit at that time, it was some person's bright idea that each production element should make its collection assets available for use by other production elements (mainly because signal types were somewhat common across element lines).

Thus, GENS, ACOM, and ALLO were instructed to send a representative to this new element (COSA or COLL) where they would perform as brokers for other elements tasking on their positions. Although the element was formed, the people remained attached to their supported organization, while the chief of the collection management shop was an independent manager.

This fact soon caused many problems, the ultimate result being the permanent reassignment of all detailed collection managers to the collection management element. Another factor was our lack of computer support as we know it today. All tasking records were maintained on 5x8 cards and a recap of this file was made (typed, proofread and mailed) every month. This file was considered the authority for all tasking, and each mission change was entered on the appropriate station/position

card as it was being forwarded to the collection site by message.

This whole process was performed by a number of typist/record keepers and collection managers performing what would be considered manual labor in today's computer world. A high percentage of positions remained tasked against a single entity (this was based on the collection site location); however, it was not impossible or unusual for several types of tasks to be assigned to a single position. A collection manager would review the tasking assigned to a station/position, look at the collection statistics received electrically from each station, and ultimately determine the best place to assign a new task to obtain the desired results.

Even at this time, most assignments were pre-directed by traffic analysts who for one reason or another (i.e. availability of linguists or on-site reporters, etc.) would tell the collection manager where the task was to be assigned. In such cases, the collection manager would ensure that the position was being manned in accordance with tasking requirements, and that traffic forwarding instructions were complete, that technical support (TEXTA) was on station, and that the new mission was not going to interfere with the task of another office.

Collection assets seemed to be plentiful and there were many more [redacted] sites around the world than there are today. All in all, our world at that time was simple with no real lack of resources. The Morse and non-Morse General Search efforts (i.e., constantly looking for new and/or unidentified signals) seemed to keep us up with what was happening in our simple world and there were people around willing to perform manual tasks.

To step through time, we remember the introduction of computers into NSA, the loss of many collection sites around the world, the many new signals that are continuing to surface, the trend to use more line-of-sight transmission systems, the lack of money, the introduction of sensitivities into our work environment, the construction of collection positions to intercept a single type of signal, communications security awareness on the part of our targets, and the changing political world of the past 25 years, all of which changes have greatly altered the role of a collection manager.

Today's collection manager is not determining where to assign a case for coverage. He has no effective evaluative tools to use in the performance of his job. The signals environment is so complex that he doesn't understand how to collect a signal or even to know what type of equipment is required in order to collect most of our sophisticated signals. He has little authority in either the current or planned collection world. Furthermore, he is uninformed about why a task is being assigned (i.e., what is the requirement). Because of this, the collection manager today is by and large a creature of the past: a rubber stamp for conveying tasks between a traffic analyst and a collector or a resource controlling authority; a record keeper for upper management who is unable to accurately respond to questions because he is not trained to interpret the data in his files; a person who is more often wrong than right when showing initiative.

Since the early days, collection management functions were returned to the analytic offices (late 60s and early 70s) and more recently moved again to a centralized organization center. I believe this again reflects a manager wanting something from a collection manager but not being able to specifically place his finger on the requirement. I believe we need to face up to the fact that we need very few collection managers (maybe only to perform collection management functions of systems [redacted] Certain of the traditional collection management tasks should be given to the traffic analyst, and a new career field should be developed for our leftover collection managers.

The new career field should include such things as being responsible for ensuring standardization when we task resources, knowing what resources are where (in accordance with the CCP and as it is in the real world), [redacted] making sure that our collection system is ready to meet future requirements, building some type of an evaluative process which informs the system when a position is not longer productive, etc.

I still believe that day-to-day collection management of items being assigned for coverage

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

is rightfully a responsibility of each analytic office. Furthermore, I believe that we need to have some focal point in NSA for working with non-SIGINT elements that have an impact upon our collection assets , and that we need to have an element involved with watching tomorrow's technology so that we are prepared for the future [redacted] Basically, the collection system must be controlled from three points, planning and budgeting, assets versus requirement priorities, and evaluation/feedback to the planning and budgeting system.

I'm not sure that I have communicated my problem with collection management and collection managers clearly. However, I feel better now that I have attempted to address it. I would like to think that somebody will read this, and just maybe there will be a review of this situation.

In the meantime, this is your collection management fireman working on a diesel collection management system, saying so long for now. I look forward to your help with my problem.

BULLETIN BOARD

NEW LAMPS FOR OLD (U)

~~(C-CCO)~~ The Division of Cryptologic History is working on several areas of our past and needs Agency files and documents for research. The areas of greatest concern right now are:

- [redacted]
- The Cuban Missile crisis;
- The Korean War;
- [redacted]
- The Vietnam War.

~~(C-CCO)~~ If you have documents of any type on these subjects (reports, correspondence, end product, codebooks, computer runs, etc.) that have been moldering in your desk or file cabinet or that may be in storage, please let us know. We are also seeking to interview people who personally participated in these events; sometimes oral history is the only way to record facts which do not show up in files. Upon the completion of these histories the documents will either be returned to you if they are part of active files, or incorporated into the NSA Archival system to make them available for historical and technical research. Call or write Tom Johnson, Chief, T542, SAB 2 Door #3, 972-2355 about materials, and Bob Farley, at the same address, about the oral history program.

~~(FOUO)~~ Materials pertaining to other events should be sent directly to the Cryptologic Archival Holding Area: [redacted] Chief, T541, SAB 2 Door #3, 972-2268.

CALLING ALL HACKERS ~~(FOUO)~~

~~(FOUO)~~ If you have had any non-work-related experience with computer "hacking" please share your knowledge with us. Success not essential, just experience. Non-attribution, non-retribution. Please contact Joe Merchant, Operations Security Manager, P1, 963-4652.

ATTENTION FRENCH LINGUISTS ~~(C-CCO)~~

~~(C-CCO)~~ Copies of *The FRANCOPHONEGLOS* with Supplement 1, dated 15 April 1978 and classified C-CCO, are being distributed again. To obtain a copy send your Name, Organization, Building, and Room number to: [redacted] P16, HQ 8A187. Mail orders only are accepted.

EXTENDED CHARACTER SETS (U)

~~(FOUO)~~ The National Data Standards Center advises that there are international standards for extending 7-bit and 8-bit character sets and for coding the escape function which invokes a new character set. The information should be of interest to persons concerned with data transmission as well as to linguists and programmers dealing with non-Latin alphabets. Particulars are described in NDSC Bulletin #6-86. For a copy write to [redacted] P13D, at their new location, FANX II, A2B03.

DOCID: 4019706

SENIOR PROFESSIONAL CAREER PROGRAM (GALAXY) Status Report

At the request of the Director, the GALAXY Steering Group undertook a review of the GALAXY Program and program objectives. The group documented its conclusions in a revised regulation which was circulated to the members of the Board of Directors for their review prior to a presentation to the Director. The decisions resulting from this process are listed below.

CHANGE 1 - CONCEPT

Personal career development is a shared responsibility of the individual and management. A centralized program such as GALAXY should not be directive, but should provide services to facilitate the attainment of objectives established by the individual and management.

CHANGE 2 - NAME

The program will be known as the NSA/CSS Senior Professional Career Program (SPCP). The change from the GALAXY name was recommended because initial intentions for the GALAXY Program created expectations and perceptions that are no longer valid but continue to be associated with the name GALAXY. The term "mid-level" has also been dropped because it is an inaccurate description in many respects. The term "senior professional" corresponds to the Occupational Specialty Titles for GG13-15 level jobs, e.g., Senior Cryptanalyst, Senior Electrical Engineer, etc. The GALAXY name will continue to be used for the data base.

CHANGE 3 - REGULATION

NSA/CSS Reg. No. 32-9, dated 11 April 1984, NSA/CSS Mid-Level Career Management Program (GALAXY), is superseded by a new regulation entitled NSA/CSS Senior Professional Career Program, dated 7 May 1986. In addition, a Personnel Management Manual (PMM) Chapter ~~410~~ 430 has been drafted and will be published shortly.

CHANGE 4 - ADVERTISING

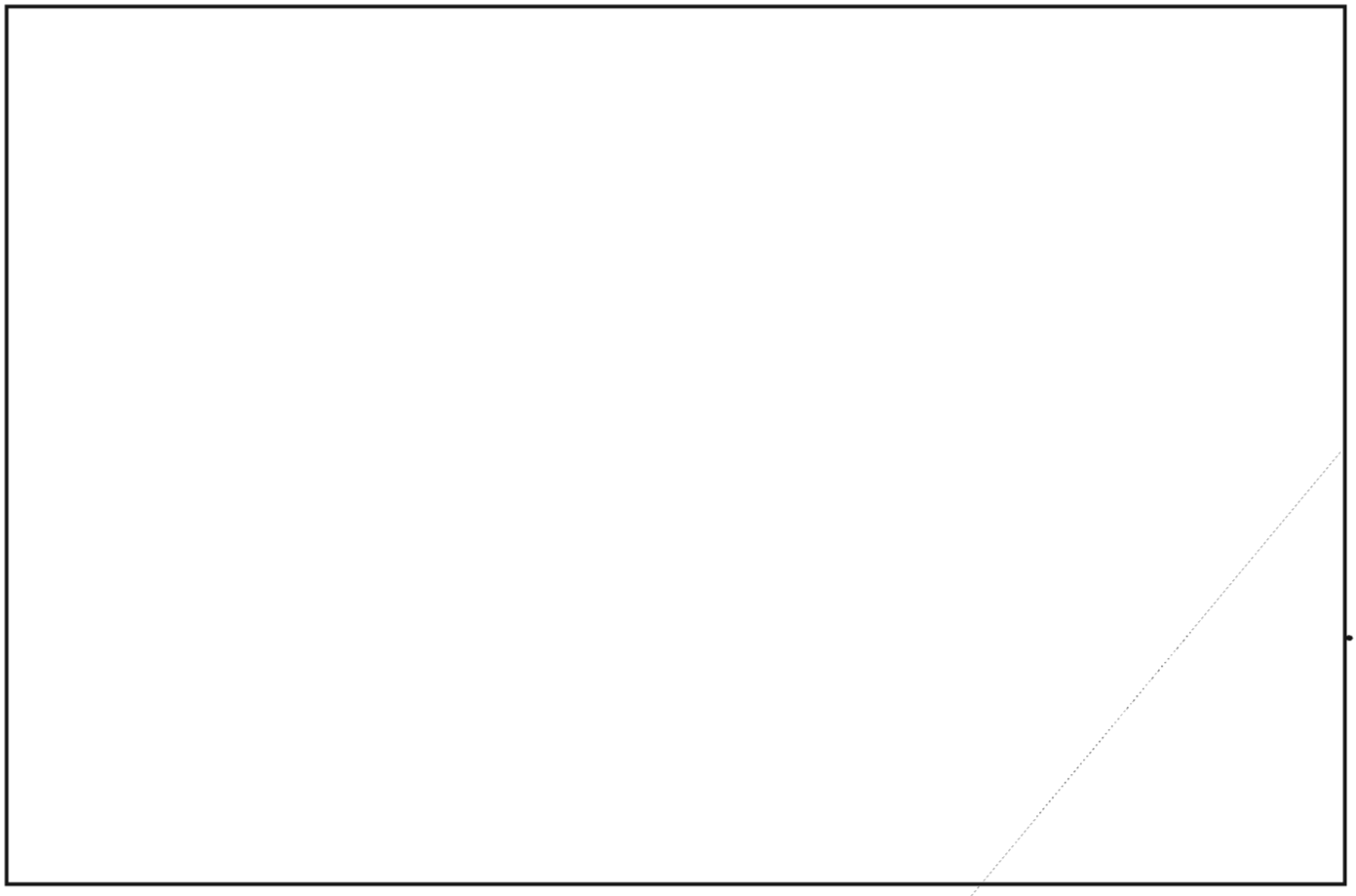
The new regulation establishes a requirement for advertising vacancies to be filled at Headquarters when the selection official desires to consider candidates from outside his/her organization. Managers can rotate personnel within their own organizations without advertising, but the job must be advertised before a cross-organizational move is approved.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

UNCHANGED

The program will continue to apply to civilian personnel at the GG13-15 level. Emphasis on field support and reassimilation is reenforced. Services will continue along present lines: maintaining data bases; publicizing vacancies; searching for candidates; coordinating selection; release and approvals; acting as focal point for field staffing and reassimilation for GG13-15 jobs and people; providing guidance and information on career opportunities and career planning.



P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

QUESTIONNAIRE #1 UPDATE

The GALAXY data base is used constantly to search for candidates to meet job requirements. You need to be as well represented in that database as possible. Please take a fresh look at your answers to Questionnaire #1. We urge you to give particular attention to secondary experience. We find that many people are conservative about claiming experience other than primary responsibilities, while requirements for a search are usually stated in fairly comprehensive terms indicating auxiliary skills and knowledges desired. Don't sell yourself short on secondary interests and experience. Please send us your changes using the attached data record.

QUESTIONNAIRE #2 UPDATE

We are preparing a reissue of Questionnaire #2 which should be more "user friendly". The answer sheets have been revised and have been printed as a standard NSA form (P1201) available in supply rooms. More about this when the new Questionnaire books are ready.

POSITION ANNOUNCEMENTS

With the new requirement for advertising, we may modify our format of the Position Announcements to some extent, but we will continue to use the following guidelines: 1) we run an ad until a job is filled or until requested to delete; 2) we do not set closing dates unless requested by the selecting official; 3) generally a new job runs two issues as a narrative and then reverts to a line item if not filled; 4) We are unable to publish in unclassified form. Therefore, the trend is toward COMINT CHANNELS so we can include more descriptive information; 5) We publish at least every 2 weeks; printing and distribution take 2 weeks; 6) 300 copies of each issue are distributed in advance to Integrated Personnel Activities at the time the document goes to press.

CAREER PATHING

We are currently working with a contractor, Human Systems Technology, to develop a model for career pathing in several fields pertaining to the procurement process (ILSM, Acquisition Specialist, Contracting Officer, Business Manager). Our basic approach is to meet with representatives of these fields to document examples of career evolution, define competencies, and identify the cross-overs which have been or should be possible. The contract will be completed in June. The pathing model will then be evaluated for applicability to other career areas.

~~FOR OFFICIAL USE ONLY~~

~~CONFIDENTIAL~~

P.L. 86-36

A NOTE FROM THE PROGRAM DIRECTOR:

(U) With a couple of years' perspective on the evolving GALAXY/SPCP program, there are two points I would like to emphasize:

~~(C)~~ First, individual initiative is the key ingredient to accomplishing a job change. Probably the greatest disservice of the GALAXY Program was to suggest to people that the Program would do it for them. We have found this is too much like playing the lottery. There are some winners, but with [redacted] GG13-15s there are a lot of people who never get called. On the other hand, a high percentage of people who want to move and take the initiative to work with us and with their supervisors are able to find a suitable new job within a six-month period. It takes persistence and patience, talking with a number of people, and waiting for selection officials to make decisions. It's a process that will test one's resolve, but the determined accomplish their objectives.

(U) Second, I consider the principal justification for our program to be to help everyone know the options. The Agency is just too large for individuals and managers to know all the posibilities. This lack of information inspires both hope and frustration. There is a sense that the "right job" or "right person" is out there somewhere if the decision-maker could only know all that is available. To a considerable extent these are not false hopes, and a brokerage service of some kind is really needed to help individuals and managers attain their objectives. We are continuing to develop all the means we can to meet information needs--advertising jobs, advertising people, candidate searches, career counseling and advice, career pathing guidance, etc. We welcome your suggestions as to what would be most helpful to you.

[redacted]

P.L. 86-36

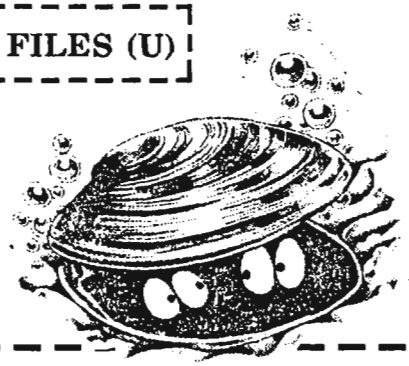
~~CONFIDENTIAL~~

DOCID: 4019706

P.L. 86-36

ASTW SHELLS TO BACK UP FILES (U)

[redacted] G743



In our office we have large number of text and data files on ASTWs. For back-up, we generally copy each file kept on the hard disk to at least one floppy disk as well.

Yesterday afternoon one of the analysts on my team, tired of typing **doswrite -afilename filename** for each file, asked if there weren't an easier way to dump multiple files to the floppy disks. After a little thought, the two of us wrote two shells.

• ① The shell **writeall** will write a list of files from the current PC/IX directory to the DOS floppy. The shell **writeall** is as follows:

```
while test $1
   do
         echo "writing" $1
         doswrite -a $1 $1
         shift
   done
```

To use **writeall,** enter one of the following commands:

```
writeall filename1 filename2 ...
writeall *
writeall filename.with.global.
   characters
```

• ② The shell **writesub** will write all files, except dot files, from a subdirectory of the current PC/IX directory to the DOS floppy. The shell **writesub** is as follows:

```
cd $1
writeall *
cd ..
```

To use **writesub** enter the command followed by the name of the subdirectory to be backed up:

```
writesub mysubdir
```

P.L. 86-36

Comment from [redacted]
Computer Science Editor:

This shell is useful when there is a need to write several files to floppy in DOS format, especially when several similarly named files can be specified with a wildcard.

As to the reason stated for needing this shell, however, I wonder why you don't simply use incremental dumps as described in the PC/IX Operations Handbook on pp 41-43. This will automatically copy every file that has been created or changed since the last dump (that way you don't run the risk of accidentally overlooking an important file) and back up all users of a given ASTW in a single step. Also, it runs faster than **doswrite.**

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

CONFERENCE REPORT

CRYPTO AT GLOBECOM 84

P.L. 86-36

P.L. 86-36

P13

(U) M/A COM exhibited their new Videocipher demodulator, designed for Home Box Office satellite TV relay. The company hopes that their system will become a de facto national and international standard.

(U) The encryption uses "hard" digital encryption of the audio channels and control information by the DES algorithm, and "soft" analog encryption of the lines of the video picture according to a DES key stream.

(U) The general scheme of "hard" encryption of the audio channel, with "soft" encryption of the video picture was specified by HBO in 1981 and presented at an EASCON meeting. [See "Video Encryption: A Report from EASTCOM 81" in the January 1982 issue of CRYPTOLOG.] The reason for the "soft" video encryption is to keep the bandwidth and format of the signal within the conventional video transmission bandwidth. The audio portion is "hard" encrypted because it is feasible to do it, and most of the program content is in the audio track. It was expected in 1981 that the audio encryption might be by DES, but a single 64,000 bps channels was under consideration. A surprising feature of the Videocipher is that the digital channel is at the megabit rate, with DES protection.

The Security of Videocipher

(U) If Videocipher is adopted as an international encryption system, which is likely since the basic scheme can be adapted to PAL or SECAM, it may be possible to limit use of DES, but there are other secure algorithms that also present difficulties.

Implications for NSA

(U) In addition to the entertainment broadcast application, the Videocipher unit can also be used for video teleconferencing --- a growing market. If it catches on for teleconferencing, the sales and dissemination of the technology could grow considerably.

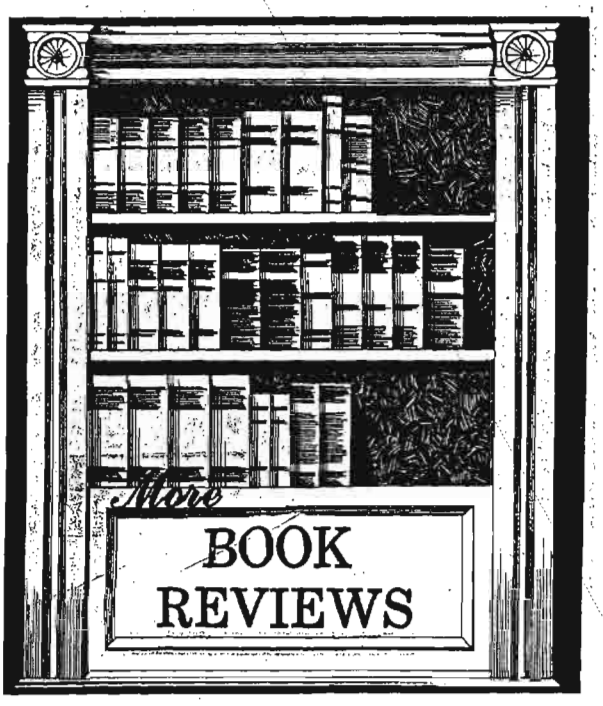
Sorry about that!

Bugs in the new software leave widows and orphans bereft, dangle parentheses and apostrophes, and cause other violations to convention.

P.L. 86-36

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

DOCID: 4019706 EO 1.4.(c) P.L. 86-36



P.L. 86-36

SECRECY, AUTHENTICATION, AND PUBLIC KEY SYSTEMS by Ralph C. Merkle
UMI (University Microfilms International)
Research Press, Ann Arbor (c1982, 1979)

Reviewed by [redacted] *P12*

~~(FOUO)~~ Let us make it clear that this is not a book in the usual sense but a revision of the author's doctoral dissertation written under the guidance of Martin Hellman at Stanford University. As one would expect, it is an immature work showing the narrow research of one student. It is not a survey of the field as the title suggests. No library need acquire this tract.

~~(C-CCO)~~ Merkle participated in the discovery, by Hellman and his many students, of what has become known to the academic world as public-key cryptography. (Actually, these systems were first conceived at GCHQ by James Ellis in 1970.) Public-key cryptography allows "secure" communications between subscribers to a large net though they have had no previous knowledge of each other and share no key in the conventional sense. Merkle's original scheme, based on solving "puzzles," as he describes it, is "primarily of pedagogical and historical interest."

~~(C-CCO)~~ The opening line of chapter 4 states incorrectly, "This chapter describes the first public key system ever developed." Of course Merkle could not have known that, several years earlier, such systems had already been proposed by Malcolm Williamson and by Cliff Cocks at GCHQ.

~~(S-CCO)~~ Perhaps it is a normal human failing to be blindly proud of one's own ideas. The idea which Merkle and Hellman originated is that of public-key systems based on the "knapsack" problem. Their design has been discredited on the outside as the result of clever work of Adi Shamir, Ernie Brickell, Andy Odlyzko, and Jeff Lagarias. [redacted] Merkle offered a prize of $100 to anyone who could solve the Merkle-Hellman knapsack; this prize was paid to Shamir in 1982. Then Merkle risked $1,000 on the security of the "iterated" Merkle-Hellman knapsack. This too was lost, to Brickell; the work of Odlyzko and Lagarias also suffices to demonstrate the unworthiness of the system.

~~(C-CCO)~~ Merkle has not entirely missed the target. The opening sentence of chapter 1 is spot on: "Cryptography is a fascinating subject, even more so today than in the past." But he alludes to the S-boxes (unique, so far as I know, to the Data Encryption Standard) as "found in many modern cryptographic functions" (page 52). And in comparing his knapsack to the sturdy public-key system developed outside by Ron Rivest, Adi Shamir, and Len Adleman, (this is the system originally proposed by Cliff Cocks), he states (p. 48): "the trapdoor knapsack appears less likely to possess a chink in its armor."

~~(C-CCO)~~ One of Merkle's ideas is that he has created an "NP-complete conventional cipher" (the title of his chapter 8). In fact his thinking is confused in several directions. Let us set the scene. A knapsack is a set $a_1,a_2,...,a_n$ of n (large) positive integers, known to everyone. The parameter n should be chosen large enough to prevent an exhaustive analysis of the 2^n

possible cryptovariables but small enough to allow timely operation of the encipherment scheme. Instead of the usual "trapdoor" use of the knapsack, Merkle intends that the sender and the receiver share key, one of the 2^n binary n-vectors, which they use to select some of the a_i which add (as integers, not mod 2) to provide a key. That is,

$$K = \sum_{i=1}^{n} x_i a_i \text{ , an integer sum.}$$

~~(FOUO)~~ Let's think about this a little. We're intending to use this key to encipher a binary stream of data, with the usual equation $C = P \oplus K$, so that the plaintext can be recovered via $P = C \oplus K$. That means that we need an arbitrarily long key stream! Yes, Merkle is ready for us. He has in mind that the knapsack elements a_i are infinite!

~~(FOUO)~~ Aha, you think -- a storage problem: where shall I retain these a_i? Never fear, that's not necessary. Instead, the sender will generate and transmit the a_i bit-by-bit! That is, in some (unspecified, but clearly essential for security) way the sender generates the n streams (starting, of course with the least significant bits) and with every bit of cipher must transmit an additional n bits of the knapsack components. Talk about data expansion!

~~(FOUO)~~ Now Merkle makes a swipe at establishing NP-completeness of his algorithm. But it's hopeless: complexity theory just cannot cope with components of infinite length. Furthermore he admits that his "proof" fails for another reason. The NP-completeness of the knapsack problem deals with the following decision problem: given the set of knapsack weights (the a_i) and an integer B, determine whether or not there is an n-long binary vector $x = (x_1, x_2, \ldots, x_n)$ such that

$$B = \sum_{i=1}^{n} x_i a_i$$

~~(FOUO)~~ The problem we're faced with as cryptanalysts is, instead, the corresponding search problem: given B, and knowing that an x exists, find x. Merkle says, "From a cryptographer's point of view there is not much difference between these two problems." It is just such difficulties that make contemporary complexity theory generally inapplicable to cryptology.

~~(FOUO)~~ Knapsacks are not appropriate vehicles for solving the authentication problem, in which secrecy of the contents is not an issue but the recipient requires assurance of the source of the message. Typically the message m is formed and then the sender A uses some function F (which is publicly known) to "sign" the message. One condition is that A (only) knows the inverse function F^{-1}: Given m, only A can find x such that $F(x) = m$. Now A calculates the signature x and transmits x only, along with a statement that it is he who has sent the message. Everyone now has the facility to read the message $F(x) = m$. No one else knows F^{-1} so no one else could have found the transmitted x.

(U) Because knapsacks typically have a very small image space, inverses of arbitrary elements m are most unlikely to exist. That is, for a randomly chosen m, it is very unlikely that a binary vector x can be found such that

$$\sum x_i a_i = m$$

so knapsack systems are not useful for authentication.

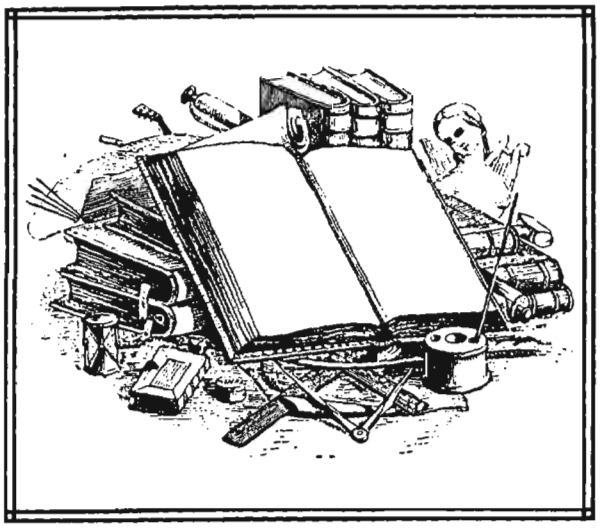
(U) Recognizing this deficiency, Merkle has written a chapter entitled, "A Certified Digital Signature." His design is "tree authentication," which is expensive, slow, and allows for the selection of only a small number of messages. Tree authentication appears again in the longest chapter, on "protocols for public-key cryptosystems," to no better effect. This chapter is not without merit: it alerts the unwary to the many pitfalls of designing secure protocols.

~~(S-CCO)~~ That Merkle fails to construct a satisfactory protocol is no disgrace: many skilled researchers have had no more success. The best work I've seen on this thorny problem has been done by [redacted] anyone familiar with their ideas will find Merkle's discussion very pale. But I particularly liked one remark of his: in the doubtful world of thrust and counterthrust, of

masquerade and tampering, the message "My secret key has been compromised" should always be accepted as a valid message.

(U) No book on cryptology is complete without mention of the Data Encryption Standard. Merkle has a novel approach to DES. He shows how to simulate a k-input m-output S-box by a knapsack with $2^k + k + m$ components. By assembling components he is now able to argue that a general algorithm which could solve a 10000-component knapsack could be used to solve DES. In a later chapter he discusses "the security of multiple encryption" of DES.

~~(FOUO)~~ Our criticism of this book is not intended as a criticism of the author. It would have been surprising indeed if such a young and inexperienced student had made an important contribution. He has not. Cryptography remains a fascinating subject, yes, but also a decidedly difficult one. □



THE COMPUTATION OF STYLE: An Introduction to Statistics for Students of Literature and Humanities. by Anthony Kenny Pergamon Press, 1982

Reviewed by [redacted] *P12/G422*

(U) Stylometry is the use of statistics in literary analysis. *The Computation of Style* is not and does not claim to be an introduction to stylometry, but it provides enough stylometric anecdotes to whet the reader's interest, such as its use in determining the authorship of certain of *The Federalist Papers*.

(U) Rather, the book intends to be an elementary introduction to statistics for those who wish to make use of statistical techniques in the study of literature. In this, the book succeeds fairly well, although a good deal of mental agility is demanded of the reader. (For example, the term "unimodal" is first used, without definition, several pages after "bimodal" is defined.)

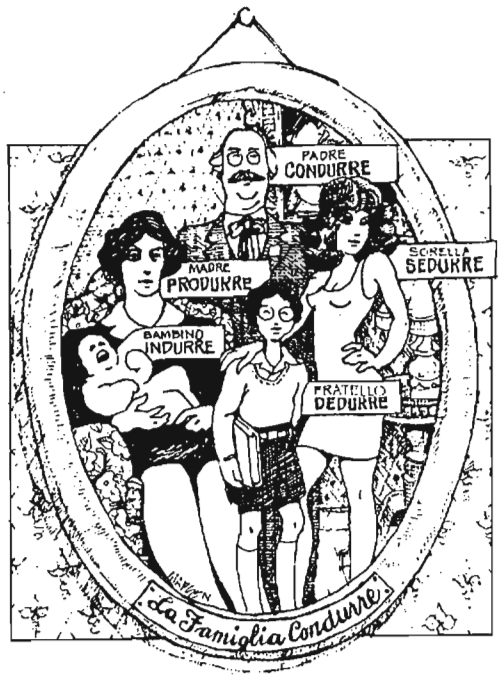
(U) The book is thoroughly British in orientation, which the American reader might find refreshing, although certain analogies such as the relationship of [highway] M6 to Manchester may be unhelpful. Passages excerpted for literary analysis are themselves a delight to read, such as two accounts of the murder of Richard III's nephews, one of which uses "the" more than twice as often as the other. The "distinctiveness ratio" could in principle be used to show that one of the authors is more likely than the other to have written a passage of unknown authorship.

(U) Most of the concepts present in the book are used to a greater or lesser degree by the cryptanalyst, such as chi-square, binomial and normal distributions, standard deviation, standard errors, significance testing, and sampling, to give only a partial listing. The cryptanalyst who wishes to review such concepts or approach them from a fresh vantage point would do well to consider this book.

(U) The author correctly states in the preface that a linguist with "a rusty memory of junior school arithmetic and algebra" should be able to follow the ideas of the book and perform the calculations needed to solve the examples. Practical applications of the techniques require the use of a calculator, or, preferably, a computer and therefore the ability to program a computer. □

P.L. 86-36

DOCID: 4019706



Drawing from Chapter 5
Verbs and Their Families: A First Approximation

P.L. 86-36

ITALIAN FOR EDUCATED GUESSERS: Shortcuts to the Language. by C. Peter Rosenbaum, M.D. Forza Press, Menlo Park, CA, 1985, $12.00. [PC 1112 .R6]

Reviewed by [redacted] *P16*

~~(S-CCO)~~ A fun book on language with short cuts for educated guessers? That's for us, the linguists at NSA! With this book (and a conventional grammar) an experienced operational linguist or cryptolinguist can slide into Italian from French or Spanish, or make the leap from long-forgotten Latin.

(U) It's an unusual size for a language book, 8 1/2" x11" x5/8" , with an appealing cover that invites you to pick up the book and peruse it. As you open it you notice that it has an attractive layout and a good "hand" -- cream-color high-quality paper that is erasable, which is a good thing, as it is a workbook. Margins are wide, and there's room for notes in the well-spaced text. But it is also a readable book that you can curl up with. And chortle over. You have to restrain yourself from interrupting your co-workers with "Look at this!"

(U) Each chapter starts with a humorous sketch illustrating the topic. (My favorite is shown on the left.) The information is logically presented, with an air of joyous discovery. Imagine coming upon "Regular Irregularities" *and* "Irregular Irregularities"! And some captions evoke operatic arias: "Unfaithful Cognates." "Unvarying Feminines."

(U) What makes this book rare and wonderful is the focus on semantics. The author takes you on a guided tour of syntax and grammar and points out the relationship between structure and meaning. This kind of analysis usually is the preserve of hard-core linguists. And the author presents the clearest exposition of sequence of tenses that I can recall.

~~(S-CCO)~~ We could have used a Spanish equivalent of this book when Cuba became an important target right after the missile crisis. There were very few Spanish linguists on board then, and even fewer lexicons and other language aids in Spanish. We made do at first with experienced French and Italian linguists who shared the few Spanish grammars and used French and Italian dictionaries. These linguists were able to walk in on the structure, and fortunately, most were also cryptolinguists and so were usually successful in finding an appropriate rendering by on-the-hoof "bookbreaking." But translating at one remove from a related language is fraught with peril. False friends abound between related languages. A special usefulness of this book is the tidy lists, with explications, of faithful, quasi, and unfaithful cognates.

(U) Dr. Rosenbaum, a professor of psychiatry who claims not to be a linguist, modestly assesses his labor of love as a supplement to a standard grammar for persons who have completed one semester of college Italian, and suggests that it might be "particularly useful for people who will be spending time in Italy." By the time you've worked through two fun-filled chapters, you find yourself *planning* a trip to Italy, just to try out your do-it-yourself Italian! □

DOCID: 4019706

To the Editor:

~~(FOUO)~~ One purpose of CRYPTOLOG is to stimulate controversy. On that basis alone, the article on ODYSSEY/CAMS [May-Jul 1986] was worth publishing. Is there anyone out there critical enough (and aware enough of its shortcomings) to critique the process?

[redacted]

~~(C-CCO)~~ Also, I consider dubious a process which does not include an interactive editing process very early in the game.

[redacted]

It would be interesting to get the reactions of the cryptanalysts who use ODYSSEY/CAMS.

'A Retiring Cryptanalyst'

To the Editor:

~~(C-CCO)~~ The ODYSSEY/CAMS article [May-Jul 1986] is both fascinating and scary. The success of this procedure is obviously directly dependent upon the quality of the original data base. Therefore, it behooves the prospective user to either clean up the data base (interactively) first, or to make sure that the data loss occasioned by this procedure is acceptable. Users who do neither should not be surprised if the cryptosystem doesn't read when it should.

[redacted]

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

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

~~(C-CCO)~~ There is no question that automation is the way to go. But it seems to this cryptanalyst that some of the procedures should be carefully evaluated before ODYSSEY/CAMS becomes the universal processing method. Instead, the designers should work with analysts in the operational areas to evaluate individual needs and to develop better initial processing procedures.

~~(C-CCO)~~ Certainly, any data base should be quickly scanned for identifiable/exploitable items which could be extracted at once. But there must always be provision for extensive cryptanalysis on resistant systems and for diagnosis, even in a paperless environment. This might mean making many printouts, or even resorting to cross-section paper and consulting the the original raw traffic. (Conversely, cryptanalysts who have worked exclusively in a paper-and-pencil mode should try mechanizing some of their efforts.)

'An Old Timer'

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

To the Editor:

~~(S-CCO)~~ I believe that Mr. Hopper's idea for organizing a workforce for C3 analysis [May-Jul 86] is right on target.

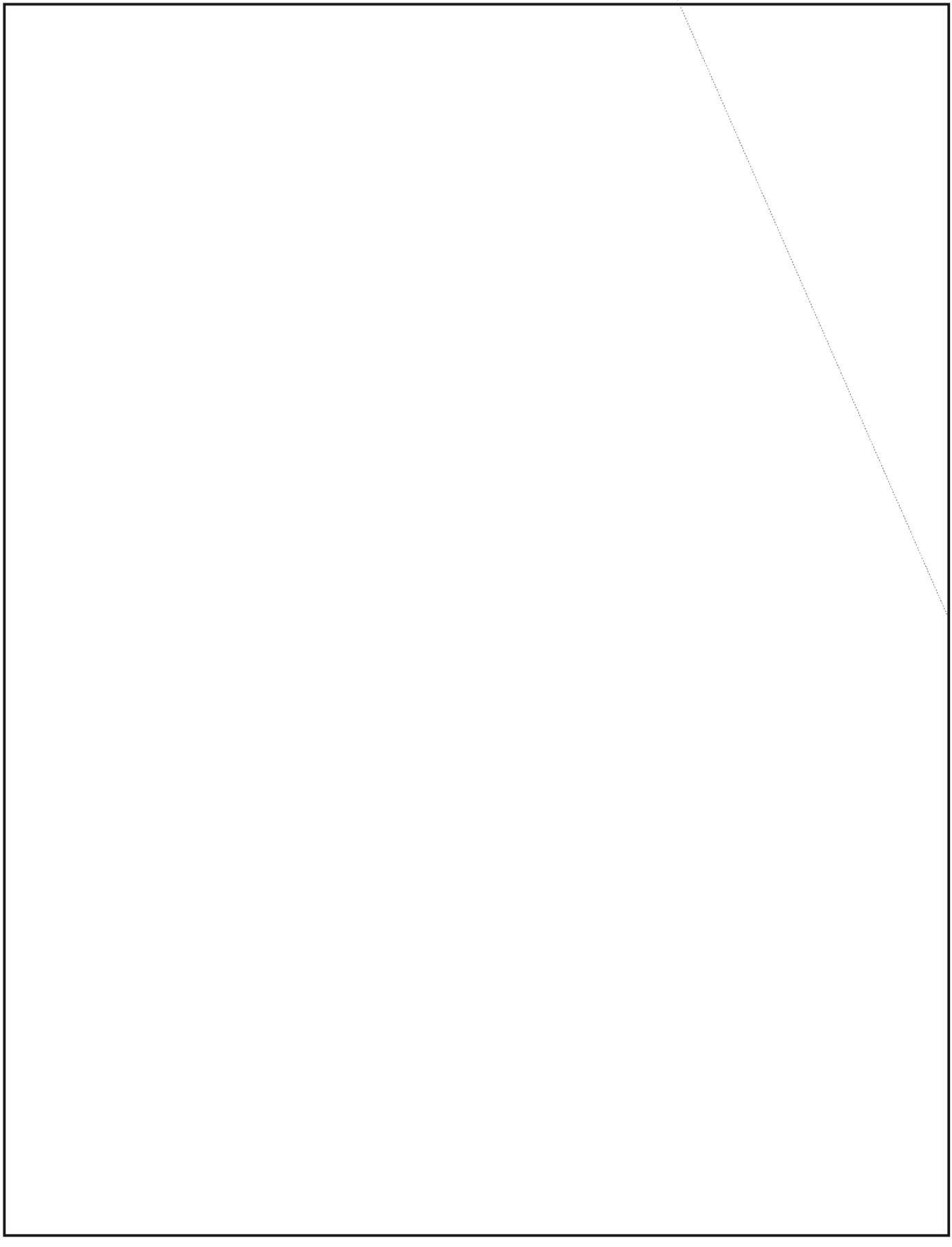
P0411

P.L. 86-36

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

DOCID: 4019706

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



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

~~CONFIDENTIAL~~

~~CONFIDENTIAL * HVCCO * NO CONTRACT~~

P.L. 86-36

~~*The following letter is classified FOUO in its entirety.*~~

To the Editor:

A short time ago I received a telephone call from an exasperated analyst in the CIA. She was interested in a report which had just been issued by NSA, but, after several calls to B and G Group personnel, she had been unable to locate the author, or even the organization to which the author was assigned. The subject of the report touched on the problem which I work, and so she had been directed to me for assistance.

Her description of the report revealed that it was a G Group product. After answering some of the analyst's questions and giving her references to two additional reports (one a CIA product she had not seen) pertaining to the subject in which she was interested, I contacted

~~CONFIDENTIAL~~

~~HANDLE VIA COMINT CHANNELS ONLY * NO CONTRACT~~

DOCID: 4019706

G05 and eventually got the name and telephone number of the author for her.

In all it took the CIA analyst and me seven telephone calls and perhaps a couple of hours to locate the author. All that time and effort could have been saved by the simple procedure of including the author's name and telephone number on the report.

In 1978 I published an article in CRYPTOLOG calling for by-lines listing authors' names and telephone numbers on NSA reports, something that sister agencies commonly do. I suggested that analysts naturally will do their very best if they know their names will appear on their product, and that the psychic income of seeing one's name attached to one's work is no small incentive to excellence.

A senior official responded that by-lines are not acceptable because of the need to maintain anonymity and because "two or more analysts often contribute to a report." My view is that anonymity can be a means of avoiding responsibility and that there generally is enough blank space preceding a report for the names of more than one analyst.

At any rate, nothing was done. However, the recent incident I referred to is common, and demonstrates again the need to reconsider by-lines to make it easier for our internal and external customers to get back to the originators.

While I believe that by-lines is the best answer, at the very least we should list a telephone number and the issuing organization's designator where a customer can contact the author. That simple procedure could save hours of unnecessary searching every year.

[redacted]

P.L. 86-36

From the Editor

IN ANSWER TO YOUR QUESTIONS

§ There are still <u>two</u> general classified periodicals being published in the Agency. **CRYPTOLOG**, the one you are reading now, is an informal monthly (bimonthly since the cuts) sponsored by DDO and published under the auspices of P1 for analysts in, or concerned with, Operations. It superseded four publications: *KEYWORD, DRAGON SEED, QRL, and COMMAND.* **The CRYPTOLOGIC QUARTERLY** (CQ), published by T54, is a formal Agency-wide vehicle for technical articles in all disciplines. It superseded two publications: *The NSA Technical Journal,* and *The Cryptologic SPECTRUM.* The editor of **CQ** is [redacted] T541, SAB 2, Door 3, 972-2355.

P.L. 86-36

§ Results of the Readers' Survey will be published in the next issue. We're allowing time for responses from the field.

§ More on OUT OF MY DEPTH #4 next time. Some readers wanted more of a challenge, so we obliged. But it's much too difficult.

§ Beginning with this issue CRYPTOLOG will be the new standard size, 8½ x 11.

Readers are invited to comment on letters and articles published in CRYPTOLOG and on other subjects of general interest.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

A PRIVATE GERMAN CIPHER OF WW I

Contributed by [redacted] *A204*

FELD=POST

HORNIST MART. WIRTH

7. INF. REGT. 3. KOMP.

1. ERS. BATL. BAYREUTH

STAMMBACH, DEN 24. MAI 1915

632B29 719T38!

B38.G2ST298.G18Z.G5T

71CH.H15S2G2K47728.S38D

V48.N252719KT.B3S.H237

2.K6SS2.G2F1H928.B38

H25T2.G18Z.A5FG292GT

61SS2.92CHT.B16D.2TW1S

V48.D39.H4̈928.4D29

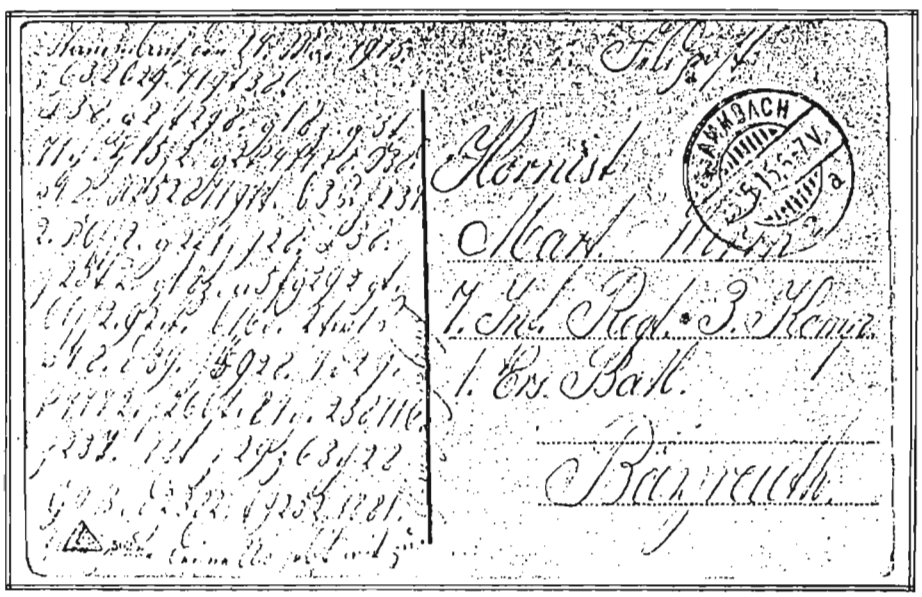
K4772.S26BST.84CH.238716.

H237.73T.H29Z63CH28

G9ß.D2382.T9252.1881

HABE HEUTE DEINE UHR SEBST MIT

ZUM UHRMACHER GEBRACHT



~~FOR OFFICIAL USE ONLY~~

DOCID: 4019706

[From]

ABS(ENDER) HORNIST WIRTH

1. ERS(ATZ) BAT(AI)L(LION)

7. R(E)G(IMEN)T 3. KOMP(ANIE)

BAYREUTH FELD=POST

AN
FRAU ANNA WIRTH
IN STAMMBACH
HS. NO. 83 OBF

BAYREUTH, DEN 23.1.1916

632B2.1881.

D238.W29T2S.KÏ9TCH28

73T.F925D2.29H16T28

B23.58S.3ST.D1SV2TT29

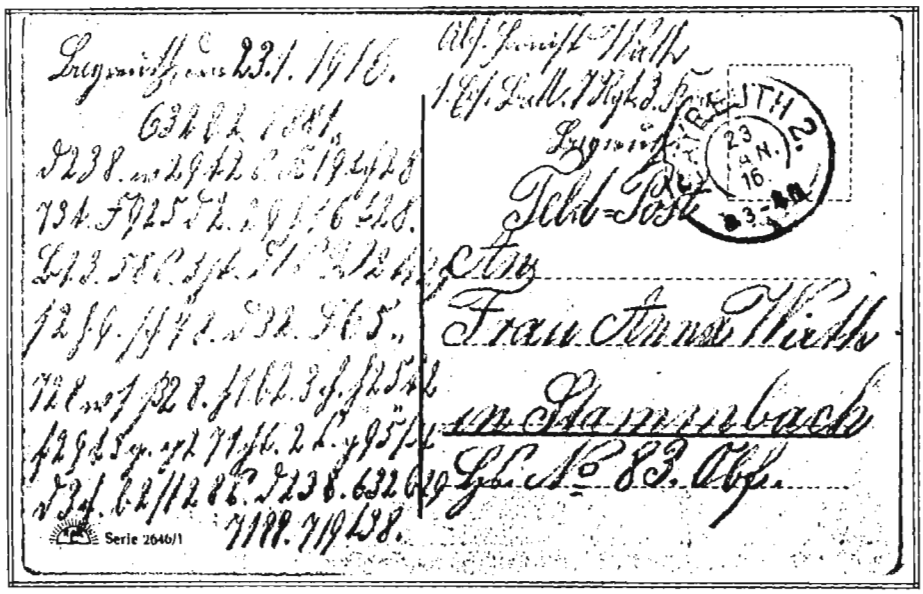
S2H9.SCH4̈8.D32.BG5

72W1SS28.H1B2.3CH.H25T2

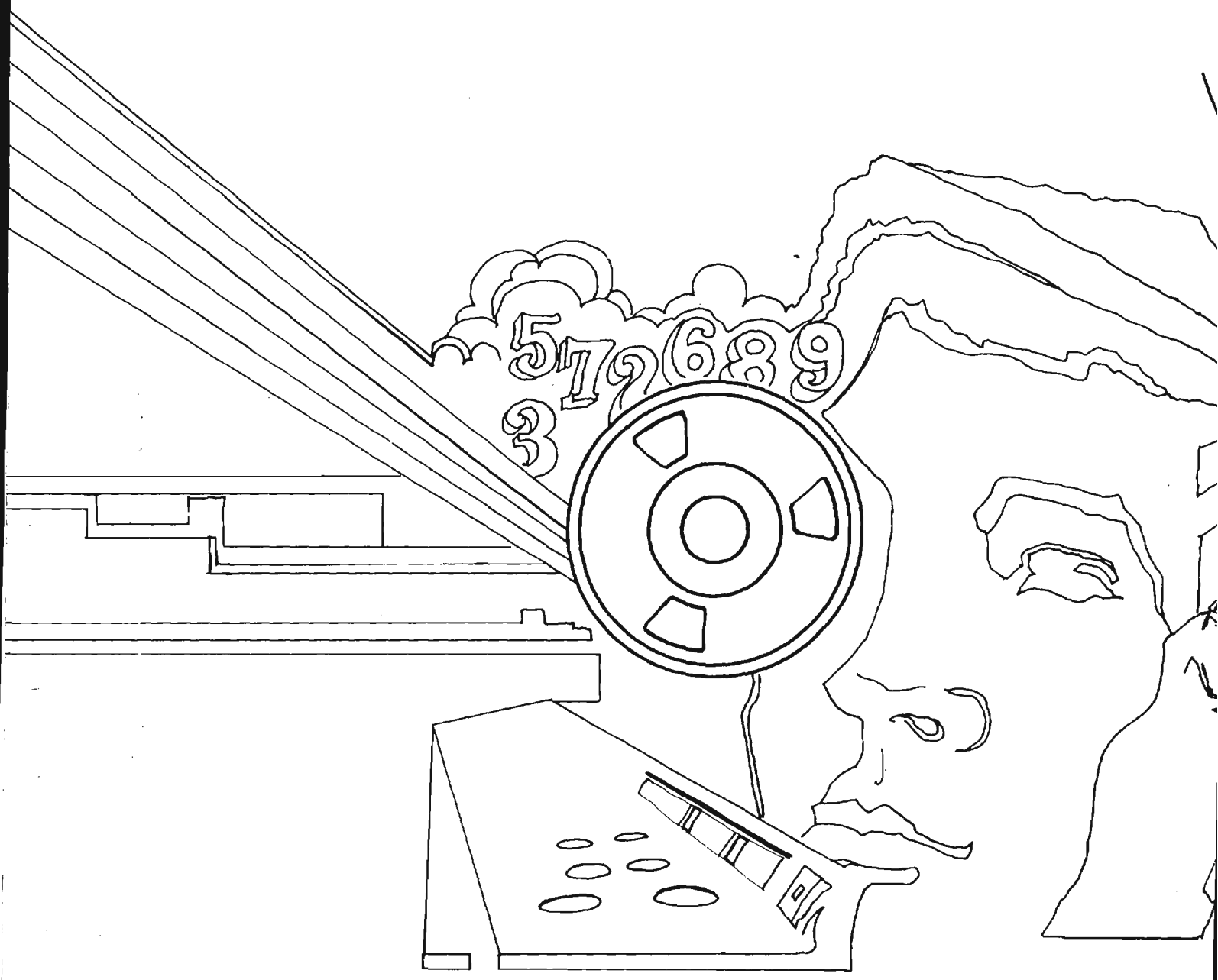
F29T3G.G271CHT.2S.G9̈5SST

D3CH.B2ST28S.D238.G32B29

7188.719T38



~~FOR OFFICIAL USE ONLY~~



~~NOCONTRACT~~