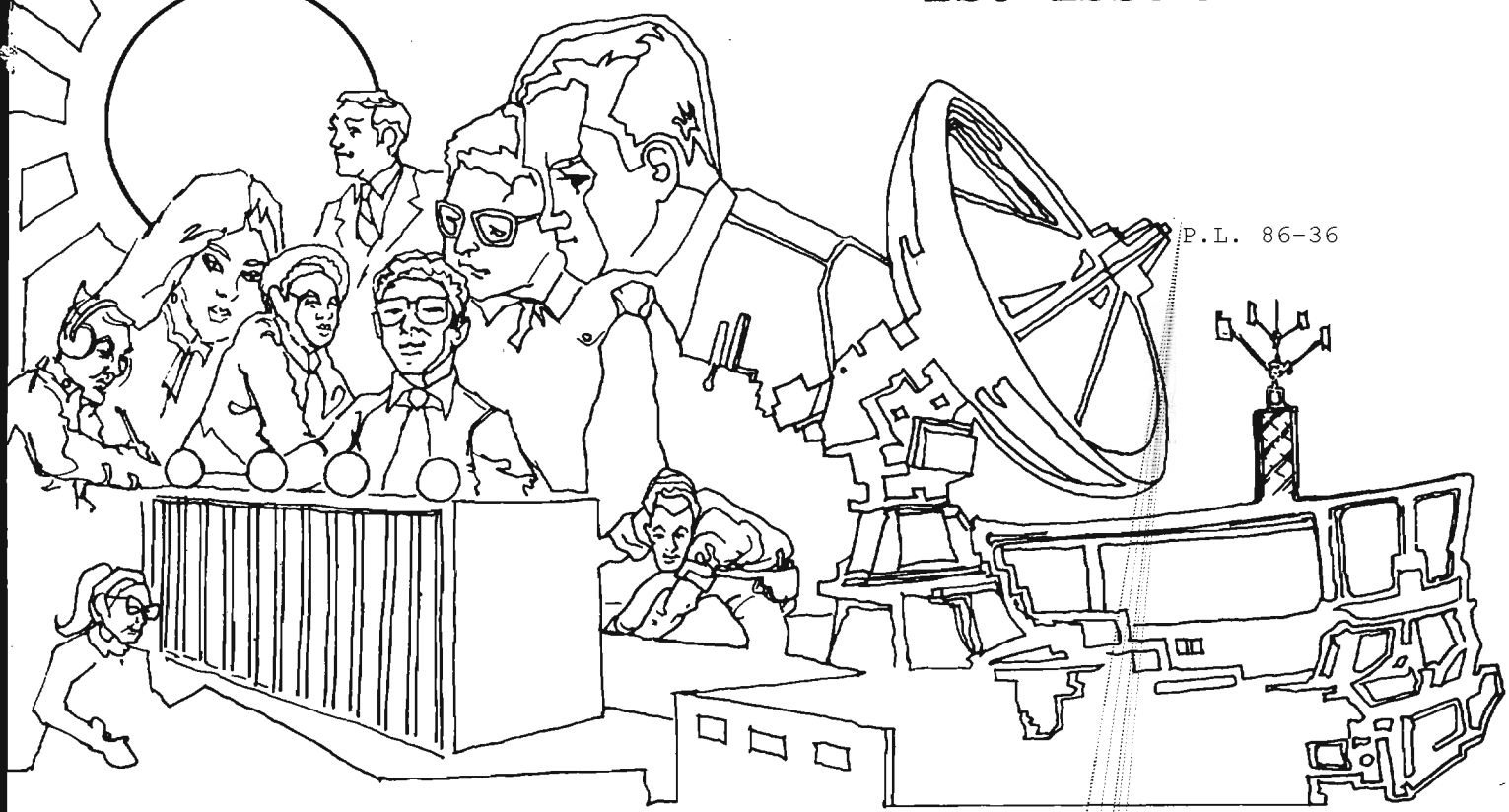
~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

1st Issue 1990



P.L. 86-36

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

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

~~NOT Rreleasable TO CONTRACTORS~~

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XVII, No. 1 ..... 1st Issue 1990

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-5238)
Cryptolinguistics ..... (963-4385)
Index ..... (963-4814)
Information Science ..... (963-3456)
Language ..... (963-3057)
Mathematics ..... (963-5566)
Puzzles ..... (963-6430)
Science and Technology ..... (963-4958)
Special Research ..... Vera R. Filby (968-5043)
Traffic Analysis ..... Robert J. Hanyok (963-4351)

Illustrators ..... (963-6234)
..... (963-6423)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, NORTH 2N018

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:
cryptlg@bar1c05
(bar-one-c-zero-five)
(note: no 'o')

via ALLIANCE, send to:
PLBROWN [note: all caps]
attn: CRYPTOLOG

Always include your full name, organization, and secure phone; also building and room numbers.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1, NORTH 2N018
Please do not phone.

A LESSON FROM AN ARCHEOLOGIST

At a recent meeting of archeologists a foremost member of that tribe made some pronouncements that astounded his fellow professionals:

- He would not appoint anyone to head a dig who could not write and communicate with the public;
- An archeologist who fails to publish (and in good time) is a destructive treasure hunter, not a scholar;
- The one-man-one site philosophy is obsolete.

Then he announced that he was stepping down as the head of his dig to devote himself to writing up earlier excavations.

Now this is bound to have a stunning impact on the conduct of all archeology, for this man directed the excavation of one of the most glamorous finds of recent times. As well as being one of the most respected archeologists ever and the author of seven books and over 100 articles -- all eminently readable -- he has appeared on television and is almost a household name. He could have stayed on, as most others have done, to bask in glory as monarch of a prestigious site.

Instead, he is using his standing to set an example for others, to write up what he had done as a junior when he was not in control of his endeavors.

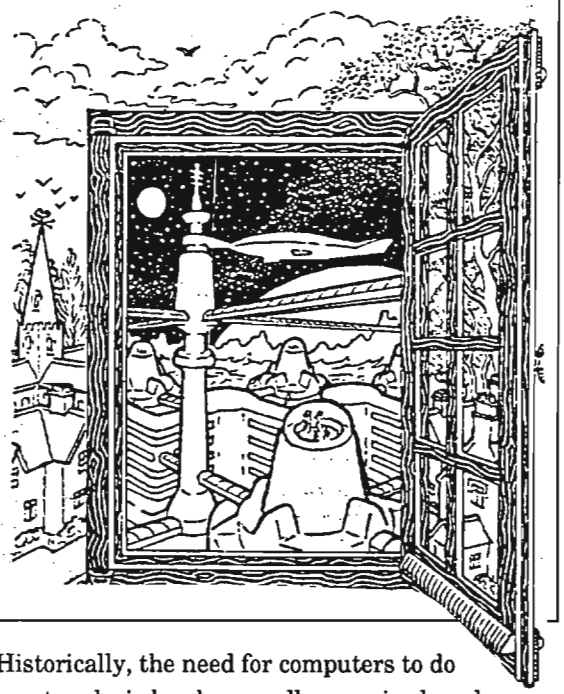
He emphasized that the head of a dig must be able to communicate, both orally and in writing, with the public as well as fellow archeologists, for it is the public who supports archeology. And it does not do to hoard your findings to write up upon retirement -- you might die before then (this has happened) -- and in any case, the information you are withholding until perfection is reached may be just what's needed elsewhere, and right now. And you certainly shouldn't spend 40 years refining references and footnotes.

As for one-man-one-site-- teamwork is what is needed by a number of specialists--botanists, anthropologists, epigraphists, geologists, pathologists, and so on. No one person knows it all.

A good example for us all.

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

BRAVE NEW WORLD



Gerald A. Young, D/Dir

This article is based on the keynote address delivered at the CRYSCO '89 Conference, 19 June 1989

CRYSCO-89 is the sixth annual Cryptanalytic Software Conference. Its theme is "Brave New World." This represents one of our more important efforts to exploit the potential of a new computer environment for cryptanalytic work.

But before I speak about computing, let me first say a few words about the importance of cryptanalysis to this Agency.

Since becoming Deputy Director, I have spent a considerable amount of time working with the cryptanalytic community as Chairman of the Cryptanalysis Council. I echo and applaud Vice Admiral Studeman's characterizations of the disciplines of cryptanalysis and cryptomathematics, along with their primary support discipline of computer science, as the bedrock of this Agency's mission. I further believe that the way we in the CA community meet the challenge of working in this "Brave New World" is critical to this mission.

Historically, the need for computers to do cryptanalysis has been well recognized, and as a consequence, the cryptanalytic community has continually encouraged the computer industry to produce ever faster machines with more computational power. We have also asked for increasingly "user-friendly" systems with ease of access and data transfer. In fact, for some previous generations of computing machines, NSA needs have been the primary driving force for development. Very early on, we used punched cards and paper tape for both program code and data media. This was followed by the use of dumb terminals for programming and magnetic tape for data, and now we have progressed to smart terminals and electronic links for moving data from machine to machine. Each change brought an improvement in some aspect of our computer resources — sometimes in the form of better response time, sometimes in the form of a more flexible input-output scenario.

In the past, with technology relatively simple compared to today's standards, we developed [redacted] our own operating system, specifically to meet the cryptanalytic challenge. [redacted] has provided outstanding editing and

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

~~CONFIDENTIAL~~

computational capabilities since its inception in 1970. [redacted] The differences caused great difficulties in software exchange and maintenance, and for years we had an environment in which this exchange was very complicated and sometimes impossible to implement. So with the arrival of Cray machines, a conscious decision was made to keep the NSA and [redacted] systems compatible. The formal accord stated that the two Agencies should jointly develop the operating system and utility software. [redacted] I believe that the success of the [redacted] effort is a prime example of skilled people working together cooperatively toward a common goal.

P.L. 86-36

The introduction of stand-alone personal computers removed the need to access mainframes for word processing tasks, but cryptanalytic work on the PCs was less successful owing to an inability to load data easily and to access data bases. However, PCs did point the way forward, demonstrating facilities such as graphics displays, color displays, and local quality printing.

Now let me move to on the present challenge.

We can no longer afford the manpower resources to modify and maintain our own operating system for each individual computer type. There has been an explosion in computer technology. Today we can — and do — network a variety of machines, linking PCs, High Performance Workstations, MINIs, and supercomputers with all types of peripheral equipment, and each component with a different architecture. But all of the new computers — the High Performance Workstations, the MINIs, the SUPERMINIs, and the supercomputers — run a UNIX-based operating system. In view of this, from a management perspective at least, it seems reasonable to move [redacted] to the UNIX operating system.

We realize that this is not going to be an easy transition, especially for those of you who are so familiar with and who have grown up with [redacted] We in management are also aware that resources are currently diverted temporarily from traditional cryptanalysis to learning the C programming language and the UNIX operating system and to converting applications programs. I realize that this is a cumbersome process. But I encourage you to look to the advantages that the new environment offers, and to devise ways to exploit its potential.

P.L. 86-36

You are already beginning to do some CA work on the High Performance Workstations, and special boards are being deployed to do even more complex tasks on the SUNs. As you gain UNIX experience, if you see inefficiencies or deficiencies, point them out to your management and work with the T organization to correct them. Together, we should be able to meet this challenge and refine the system to do an even better job than we have in the past

With the variety of computer resources available to you, I challenge you to find appropriate uses for each of the capabilities, to identify the right machines for a particular task, and to maximize the use of this vital, versatile wealth of computer power. To that end, I fully support the goals of the Cryptanalytic Software Conference, together with the year-round work of its sponsoring organization, the Cryptanalytic Software Committee.

I also see that the conference agenda includes a session where each of the major crypt organizations describes its progress in meeting the challenge of adapting to the new computing environment. I encourage as many of you as possible to go and hear what others have tried, what they have developed, and what they have learned.

Share your ideas and your software! Maximize your resources! By doing so, we can meet the challenge presented by the growing number of cryptanalytic problems we see today. If we do this right, we can insure future cryptanalytic success for years to come. ❑

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

~~CONFIDENTIAL~~

[redacted] B04

P.L. 86-36

CRYSCO-89

RECOMMENDATIONS

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

This paper serves as a record of CRYSCO-89. It lists the recommendations and also some observations and comments made during the conference. While the latter are not recommendations, they should be recorded. Note that "observations" are provable statements, while "comments" are the opinion of one (or more) speakers, which you may or may not agree with.

Priorities are included for the recommendations, which will be actioned by CRYSCOM in a timely fashion during the next 12 months. A separate "Recommendation Status" list will be created - and updated - giving current status on each recommendation. CRYSCOM is a volunteer organization, and each organization is requested to share in the work load. Organizations are requested to review the "Recommendation Status" list periodically for recommendations of interest or concern which they would like to pursue.

1. MOVE TO UNIX.

Recommendation: Encourage the move to UNIX, by promoting its advantages, sharing findings, providing examples of how to get the best from UNIX, etc. Discuss advantages and disadvantages of using pipes.

Priority: High.

Observations: UNIX has increased productivity for some. Should do things differently under UNIX [redacted]

P.L. 86-36

Comments: Get on with the move, it's not as daunting as it first appears. People who have used UNIX heavily have come to like it.

2. SOFTWARE PORTABILITY.

Recommendation: Maintain a list of what to do to keep code portable. Establish guidelines on C and FORTRAN inter-callability.

P.L. 86-36

Priority: Medium.

[redacted]

3. SOFTWARE MANAGEMENT AND EXCHANGE.

Recommendation: Establish a mechanism for UNIX to UNIX software exchange. Agree on common conventions on how to send exchanged software; aim at software easy to install by receiving organization. Promote the use of variables (internal and environment) in "make" files.

Priority: Very high.

Comment: Get on with UNIX software exchange. Try it and see.

4. LANGUAGES.

Recommendations: Promote, explain how, etc., to get autotasking to several CPUs. Encourage discussion on the advantages of FORTRAN and C.

Priority: Medium.

Observations: Modern FORTRAN and C compilers produce code which usually runs twice as fast as IMP compiler code. C compilers are getting better, approaching current FORTRAN compiler.

Comment: IMP is being phased out.

5. WINDOW SYSTEMS.

Recommendations: Teach the terminology of window systems. Encourage use of window systems - preferably a common one.

Priority: Medium.

6. NETWORKING.

Recommendations: Promote goal of networks being transparent to users. Check that response remains good with various terminal configurations (notably SUN workstations) at peak loading. As appropriate, keep users informed of security issues.

Priority: Low.

7. HARDWARE.

8. COMMERCIAL SOFTWARE.

Recommendations: Complete and maintain catalog of who has what. Expand above to include use and evaluation of the software. Include list of people able and willing to help others use the product. Expand subject to include public domain software. Encourage progression to standard products.

Priority: Very high.

9. CRYSCOM DISTRIBUTION.

Recommendation: Distribute relevant papers, info., etc,. through CRYSCOM channels.

Action required: Each organization should inform CRYSCOM Executive Officer of changes, additions, deletions, etc., required for their organization.

Priority: High.

10. WORKING GROUPS.

Recommendation: Create working groups to study topics of interest. Provide terms of reference, timetable (2 to 3 months) and monthly reporting mechanism.

Potential subjects: Crypt techniques - what is available where. Sorts - what do we need under UNIX. System accounting under UNIX.

Priority: High.

11. TOPICS FOR UNIX BROWN BAG SEMINAR (UBBS)

Recommendations: NFS, NQS, "lex" and "yacc". UNICOS 5.0 facilities. Other system upgrades.

Action required: Present seminars once a month or as needed. Organizations to volunteer speakers for topics they can cover.

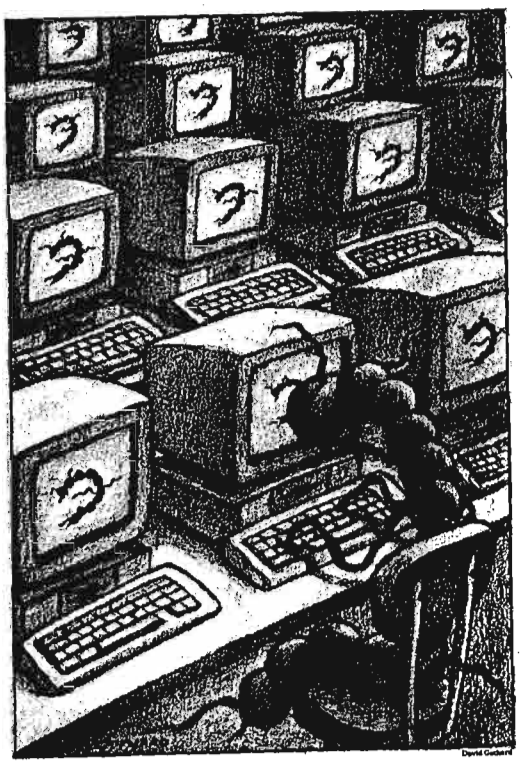
Priority: High.

12. SUPERCOMPUTER SYSTEM SOFTWARE SUPPORT.

Recommendation: Provide priorities to T335.

Priority: High.

Comments: Recognize that T335 has a lot to do and cannot do it all at once. Appreciate T335 contribution to the crypt community. ❐



THE COLUMBUS DAY VIRUS

C313

There has been public and governmental apprehension about a possible computer virus attack designed to be launched Columbus Day, October 12. Therefore the National Institute of Standards and Technology compiled information from public sources about the "Columbus Day" virus and computer viruses in general and issued a statement to the press. The statement was prepared in conjunction with the National Computer Security Center and coordinated with the Software Engineering Institute. In summary, it found no evidence that the virus has spread widely in the US.

Then C313 conducted an independent analysis of the Columbus Day virus, more properly known as the DATACRIME virus. It verified that the characteristics of the virus do indeed match those reported publicly, and will, upon execution between October 13 and December 31 inclusive, make hard disks unusable.

Concern has focused on the possibility of widespread damage on IBM personal computers and clones running the PC-DOS or MS-DOS operating systems. Most researchers on computer viruses believe that the virus in question is a member of a virus family known as "DATACRIME." Since attention has first been drawn to this virus, there has been a lot of analysis as well as public discussion on its characteristics. The results of disassemblies, along with descriptions, have been posted on electronic digests, such as VIRUS-L. Most everyone participating in these discussions has come to the same conclusions, in which C313 researchers concur on the basis of their own work.

PUBLICLY REPORTED ACCOUNTS

While the virus has been referred to as the "Columbus Day Virus," it is more correctly referred to as the DATACRIME virus. It was reportedly released on March 1, 1989, somewhere in Europe. This virus is currently reported to have two versions, of which one version also has two strains.

Editor's note: This article is based on a report released prior to Columbus Day 1989 for internal NSA use.

Reported Size / Version

One version of the DATACRIME virus has two strains which are named by the number of bytes by which the virus increases the size of infected files. One of the strains has a size of 1,168 bytes and the other has a size of 1,280 bytes. There is still another version of this virus, most often referred to as "DATACRIME II," about which little information has been reported. It is believed that its size is still larger than that of the other version.

Reported Propagation

The 1,168 -and 1,280-byte strains of the DATACRIME version propagate to files with ".COM" name extensions (with the exception of "COMMAND.COM"). The DATACRIME II version infects files with either ".COM" or ".EXE" name extensions.

Reported Mission

Both versions of the virus perform a low-level format of cylinder zero on the "C:" hard disk drive. This action will destroy disk directory information, thereby making the hard disk unusable.

Upon activation, the DATACRIME version displays the following message:

```
DATACRIME  VIRUS
RELEASED:  1  MARCH  1989
```

The DATACRIME II version displays this message upon activation

```
*  DATACRIME  II  VIRUS  *
```

Reported Date of Activation

For both versions, the mission of the virus is triggered upon execution of an infected file after October 12 (i.e., October 13 or later).

Reported Characteristic Strings

For the DATACRIME version, the 1,168-byte strain contains the hexadecimal string 'EB00B40ECD21B4', and the 1,280 byte strain contains the string '00568DB43005CD21'. A characteristic string for the DATACRIME II version has not been reported.

C313 ANALYSIS

In most cases we confirmed the reports by both static and empirical methods. Static methods included reviewing hard copy of disassembled virus code, while empirical methods included observation of the actions of the virus on isolated systems and analyzing actual code with utilities such as debuggers. The empirical methods were performed on three different systems: an IBM PC with two floppy drives, an IBM PC-AT with one high-density floppy and one 30-MB fixed hard disk drive, and an IBM PC-AT with one high-density floppy and two 10-MB removable cartridge disk drives. In several cases we were able to glean additional information that was not mentioned in the public reports.

Size / Version

Static and empirical methods confirmed that the two strains of the DATACRIME version increase the size of infected files by 1,168 and 1,280 bytes respectively. In addition, we determined that the DATACRIME II version increases the size of infected ".COM" files by 1,514 bytes. The DATACRIME II version increases the size of ".EXE" files by a non-constant number of bytes, usually between 1,500 and 1,800 bytes. Additionally, a large portion of the DATACRIME II version is stored on disk in a simple encoded format and is decoded prior to execution.

Propagation

Static and empirical methods confirmed that both the DATACRIME and DATACRIME II versions of the virus propagate to files with ".COM" name extensions, while only the DATACRIME II version infects files with ".EXE" name extensions. We were also able to clarify the report that the virus would not infect the "COMMAND.COM" file. Actually, neither version will infect *any* file where the seventh character is a "D". Additionally, both versions will infect only one file per execution, and both will infect files as long as the system date is between January 1 and October 12 inclusive.

Mission

Static and empirical methods confirmed that both versions of the virus perform a low-level format (INT 13, function 05) of the 80H

drive (usually a hard disk drive, most often named "C:"). Additionally, this operation will format up to 10 surfaces of a disk. Both methods also determined that the text strings printed by the versions of the virus match those reported in public sources. The text strings in both strains of the DATACRIME version are stored in an encoded manner instead of plain ASCII. As previously mentioned, the DATACRIME II version is almost completely encoded.

Date of Activation

Static and empirical methods confirmed that both versions of the virus will activate their mission when the system date is between October 13 and December 31 inclusive.

Characteristic Strings

Static and empirical methods confirmed that the publicly reported characteristic strings in the DATACRIME version do actually exist in the code. The 1,168-byte strain contains the hexadecimal string 'EB00B40ECD21B4', and the 1,280 byte strain contains the string '00568DB43005CD21'. Additionally, we have determined an acceptable characteristic string for the DATACRIME II version, which is 'F8C288BF26CF8F81D9'.

OBSERVATIONS

Based on our analysis of the virus and a review of related information, we have some comments on various issues that are not necessarily covered by the items of interest we have identified so far.

Development of the Virus

We believe the DATACRIME version was the first version released, because of its relative simplicity in comparison to the DATACRIME II version. In addition, we believe that the 1,280-byte strain was the first of the two strains of the DATACRIME version. While the 1,280- and 1,168-byte strains both contain duplicate code in many places, the 1,168 has improved efficiency in some places, most notably in the smaller size. The DATACRIME II version, however, has many improvements over the original DATACRIME version, in that it infects both ".COM" and ".EXE" files, and makes primitive attempts to hide itself with encoding.

Detection

There are several ways this virus may be detected. One is that there is an increased file size upon infection. Another, one of the easiest ways, is to search for the characteristic string(s) of the virus is using a tool such as The Norton Utilities**1 or the DOS DEBUG utility.

Finally, the virus may access other floppy or hard disks in its attempts to propagate. It may be detected by such unexpected accesses.

Recovery

Our analysis has shown that the average DOS user will find it difficult to recover from this virus. Both versions of the virus do a low-level format of the hard disk upon activation, which standard DOS utilities cannot overcome. The best advice for average DOS users who need to recover from the malicious actions of this virus is to seek help from a local expert on DOS.

For individuals who believe themselves capable of restoring a system, there are really two cases to consider. The first (preferred) case is where backups of critical data have been kept. The second case is where no backups have been kept, but critical data must be recovered from the disk. Note that the procedures below do not address the possibility of non-DOS partitions and systems present on the hard disk. Specific knowledge of those systems will probably be necessary to restore non-DOS partitions. We will only address DOS partitions here.

▸ *If backups have been kept, the following procedure should be used by a knowledgeable user to restore the DOS disk partition:*

1. Boot from manufacturer's DOS floppy
2. Restore disk partition table using a tool such as The Norton Utilities
3. Format DOS partition (may require an initial low-level disk format to make the disk bootable)
4. Restore all files from backup EXCEPT executables (those with ".COM" and ".EXE" name extensions).
5. Reload all executables from manufacturers' disks or re-compile local source files to produce executables.

▸ *If backups have not been kept, the procedure is much more difficult. In fact the following procedure may be more difficult than retyping text and data files by hand from hard copy:*

1. Boot from manufacturer's DOS floppy
2. Restore disk partition table using a tool such as The Norton Utilities
3. Attempt to recover critical text or data files from disk using a tool such as The Norton Utilities; note that this may require searching entire disk for data blocks related to a particular file
4. Save recovered data or text files to floppy disk
5. Format DOS partition (may require an initial low-level disk format to make the disk bootable)
6. Reload executables from manufacturers' disks
7. Reload saved data or text files

THREAT

We feel it is important to address the potential threat of this virus. To date, there have been very few reported cases of this virus in the US. Most of the interest we have seen in this country has been from a technical standpoint or from rumors in press accounts, and not from victims who have been attacked and seek a remedy. As a result we feel that the current versions of this virus pose a small threat to US systems.

Note that there appears to be no specific year associated with the actions of this virus. If an infected file is executed between January 1 and October 12 of any year, it will try to infect other files. If an infected file is executed between October 13 and December 31 of any year, it will attempt to format cylinder 0 of a hard disk drive. It would be prudent for people who detect the virus or those whose disks are damaged by the virus to look for other infected files on the floppy disks they use as well.

CONCLUSIONS

The C313 analysis has shown that the DATACRIME virus does indeed match the characteristics that have been reported through public sources. Its intent is malicious, and it will format cylinder 0 of the "C:" hard disk drive when activated on or after October 13. It is important to mention that owing to the difficulty we had in obtaining a copy of this virus, and given the comments in publicly-available sources, we do not believe that this virus has spread widely in the US. Therefore, we do not rate this virus as any more important than other currently known viruses. However, the lesson to be learned from this virus and others is that good prevention techniques need to be applied all of the time, and not just in times of reported outbreaks of viruses.

ACKNOWLEDGMENTS

The following C313 researchers participated in the analysis of the virus in and the preparation of this report:

Research material for this report was obtained from the following sources:

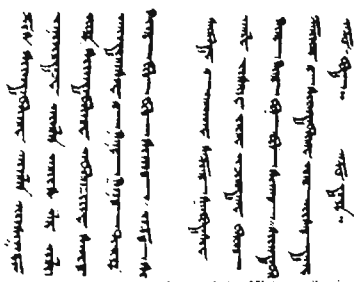
David Chess, IBM; David Brown, Department of Energy Computer Incident Advisory Capability (CIAC); Ken van Wyk, DARPA Computer Emergency Response Team (CERT).

A Note to Subscribers

The distribution for this issue reflects changes received by COB 4 April 1990

~~SECRET~~

THE CRYPTOLOGIC LINGUIST PROGRAM



UIGHUR SCRIPT. The writing of the Uignur tribe in central Asia and western China in the medieval ages. Sometimes written horizontally.

PASSEPA SCRIPT. Established by Kublai Khan in the 12th century as the official international script of the Great Mongolian Empire.

KÖK TURKI RUNES (ORKHON SCRIPT). The writing of pre-Islamic Turkic peoples in northern China about the 6th century.

[redacted] P16 P.L. 86-36

~~(C-CCO)~~ The Cryptologic Linguist Program began with the perception that there is a need to have a pool of multilinguists ready for immediate deployment against language problems as they arise, rather than to attempt to identify, recruit, and train linguists to attack a problem that has already grown to critical proportions. The concept is deceptively simple. All one needs to accomplish that end is the ability to look twelve months or more into the future [redacted] Failing that, one takes an educated guess and begins recruiting and training people in languages that appear to be the best bet.

[redacted]

[redacted]

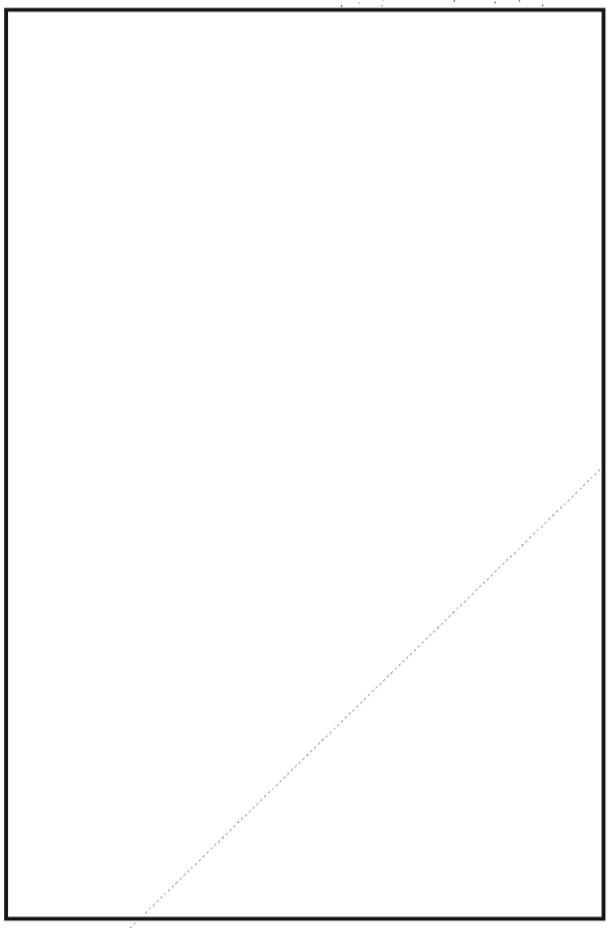
(U) As the present tendency is to follow the inclinations and desires of the individual program member in broadening the language base by family or area as long as the languages fit into the perceived needs of the Agency, all three paths are being followed.

~~(FOUO)~~ Linguists are brought into the Program through one of two paths: direct hire or on-board recruiting. Direct hires have either postgraduate degrees in a language or in a discipline that requires a strong language minor such as history or linguistics, or a demonstrated proficiency in more than one language with very high aptitude for learning languages. On-board recruiting is done by advertisement through M36 to all Agency elements. Successful candidates for entry into this three-year Program are already certified in at least one language and have developed reputations as high achievers in their assigned elements.

~~(C-CCO)~~ Administration of the Program is modeled on the intern programs, in that members are detailed to six-month tours over a three-year period (more or less), with training in language and associated skills as with interns. The major difference is that since the members enter the program with widely varied skills and backgrounds, individual goals are stressed more than common milestones. When

language skills permit, the members tour across groups (A & G, A & W, G & B, etc.) and field sites to broaden their knowledge and perspective. Graduation from the Program is contingent upon fulfilling two conditions: certification in a target language (or a new target language in the case of on-board hires), and assignment to a billet in an Operations organization.

~~(C)~~ The Program was initiated on July 1974 with a memorandum from LtGen Allen, DIRNSA/CSS. directing that a three-year program be initiated, designed to "develop a corps of cryptologic linguists performing tasks in support of the linguistic effort of the Agency, who are capable of operating effectively in several languages and to emphasize in this group the broad application and development of linguistic proficiency across the cryptologic spectrum." The Office of Techniques and Standards (P1) was directed to administer the Program, and that administration was delegated to the Languages and Linguistics Division (P16).



TO NEW AUTHORS

Once you've written your article, the hard part begins--editing your own work. A good writer is a rewriter: improving, simplifying, clarifying. Sometime stop at a library that has the ms collection of a noted author; you'll see evidence of many, many revisions.

How to start?

First, set the paper aside for a week or two "to develop the flavor" as the cookbooks say. Print it out double-spaced in a monospaced font. Review the hard copy. A little distance will give you fresh perspective. Obvious flaws will shout at you. Mark the changes in a bright color.

Fix the soft copy, reprint it, and check for wordiness. Every word or phrase should be load-bearing. Reduce "during the FY91 time frame" to "in FY91;" "at this point in time" can be boiled down to "now." Readers just will not wade through thickets of dead wood.

Reprint.

Once the text is lean, the organization of thought should be clear. Check the first paragraph. Will your point be evident to readers and invite them to read on? If not, reword it. Does it look like alphabet soup? An excess of abbreviations and acronyms is poison.

Fix it. Reprint.

Do a field test. Find a reader, a good and true friend, who will mark the text wherever there is an unclear passage, wherever something isn't just right. Take the comments in good heart. Keep in mind that not every reader is as up on the subject as you are, and might need an explanatory phrase now and then.

When you've honestly done as much as you can, send it on to CRYPTOLOG. If you prefer, you may call one of the subject editors for aid and comfort.

A Note on the Linguist Problem

[redacted] G142

P.L. 86-36

~~(C-CCO)~~ There seems to be general agreement on at least two aspects of the linguist problem at NSA: [redacted] and, linguists are leaving the language career field because they see better promotion opportunities in the management or staff career track. This has a deleterious effect on intelligence production, because most of our targets perversely persist in using languages other than English, thereby forcing us to rely on linguists to make sense of the traffic. While management stresses the importance of linguists, it does not seem to be overly concerned by their exodus since it has taken few effective steps to correct the problem. The one substantive step, the FLIP program, fails to address the problem because it attempts to substitute token premium pay for what employees really want, namely, promotions

[redacted]

collection staffs in order to enhance their careers, there seems to be some justification for this approach. One can find former linguists at all levels of NSA's management structure. They probably would not have gone as far had they remained working linguists. The fact that there are breathtakingly incompetent managers who have somehow reached relatively senior positions could reinforce the perception that the management track is a relatively easy and foolproof path to career advancement. Still, one wonders which is easier to replace, a mediocre office chief or a mediocre Hungarian linguist?

(U) In spite of the management's protests, linguists will probably continue to leave the language field as long as the current situation persists. In other words, the lack (or perceived lack) of linguists stems from certain management decisions that can only be corrected by the management. Should management bother to do that?

(U) It is obvious that we are currently witnessing profound upheavals that will shape the world situation for years to come. Since our government finds itself more and more frequently in the uncomfortable position of having to make important decisions on increasingly short notice, the need for timely, relevant, and above all plentiful and accurate intelligence is greater now than at any other time in the recent past.

~~(C-CCO)~~ Even though NSA claims to be an analytic and reporting agency, a great deal of its budget is spent on machinery and resources needed to operate that machinery, and comparatively little on analysis (including language analysis) and reporting. Even though we collect and

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

P.L. 86-36
P.L. 86-36

It seems to me that this is analogous to building the Hoover Dam in order to operate a single light bulb. The benefits derived simply do not justify the cost of the infrastructure.

(U) A better solution might be to shift some personnel (and related promotion points) from staff positions to operations. Even though they were originally intended to help the operational elements, many staffs have over time become hindrances to both operations and operational elements' interaction with customers and collectors. Not only is every operational element down to the office (and sometimes division) level liberally larded with staffs of its own, we seem to have developed a number of large, remarkably well-manned organizations dedicated to staff and protocol functions. Over time, these staffs have evolved into sequential choke points through which virtually all information coming in and out of the Agency must pass. The current situation is such that many operational elements are successful only to the extent that they are able to get around the system, often with the help of sympathetic staffers, in order to get the job done. In other words, we have invested much of our resources into a system that now forces us to expend additional resources to circumvent it. One is almost reminded of Dr. Strangelove, who kept trying to strangle himself with one hand and using the other to free his throat. In addition to streamlining operations, a reduction of staffs might even enhance security, since it would reduce the number of people who are needlessly exposed to sensitive information.

~~(S-CCO)~~ In addition to an immediate boost in the quality and quantity of intelligence production, an increase in the size of the operations workforce would create more promotion opportunities for linguists and other analysts, especially to higher grades, and retention in those fields would undoubtedly improve. Another benefit would be increased decentralization and flexibility, which would also have a beneficial effect on efficiency and productivity. Because they are more efficient and flexible, for example, private companies with decentralized operations consistently post higher profits than those with rigid central planning.

~~(S-CCO)~~ Shifting decision-making, customer relations, and collection responsibilities (and resources) to the lowest possible (i.e. analytic) level would ensure more timely, plentiful, and accurate reporting, greater responsiveness to customers' needs, and more effective coordination

It would also identify those linguists and analysts who, in addition to technical and linguistic expertise, have the background, target knowledge, mature judgment, and dedication to the Agency's mission that would qualify them for promotion to STE ranks. Better retention in the language field, and the consequent improvement in intelligence production, would go a long way toward making NSA what it claims to be, a true intelligence agency and not a mere collector. ❐

THE ROLE OF OPSEC

in improving the effectiveness of a cryptologic mission

Experience in peacetime and wartime civil and military governmental operations has shown that even where good security programs were being implemented in each of the traditional security disciplines, an adversary has been able to acquire critical information that impaired our ability to accomplish the mission.

OPSEC is an analytical discipline for improving mission effectiveness by denying to an adversary critical information that could impair the mission. The term "adversary" in this context refers not only to hostile intelligence services but also to any entity whose acquisition and use of critical information, whether or not maliciously intended, could impair the mission. OPSEC and the traditional security disciplines are complementary in that they are all directed at the protection of national security information. In the OPSEC process, however, all aspects of an operation are examined, including support functions.

THE OPSEC PROCESS

As could be expected of any analytical discipline, OPSEC has a well-defined methodology, called the OPSEC Process. It is composed of five steps:

1. The identification of critical information about the operation that must be protected.

This is crucial to the process. Operations personnel determine what specific information about an operation must be denied to the adversary lest it be used to neutralize or negatively impact on the mission.

It should be noted that the question asked is not what classified or sensitive information must be protected but what information, if obtained, could impact negatively on the mission. Called "critical information," it may be unclassified, even in classified or compartmented operations.

All cryptologic missions have information about the activities that must be protected if there is to be the best chance of success. Some examples are: the itinerary of INFOSEC inspections, the criticality of communications nodes, the specific mission and targets of a facility, degree of success.

2. Analysis of the mission-specific threat

The adversary's technical capability and resources for exploiting vulnerabilities of the operation and thus acquire critical information are assessed in this step. Included in such threat assessment must be a realistic appraisal of the adversary's opportunity and intention to undertake such exploitation, the risk it subjects itself to in the process, and its willingness to accept the risk.

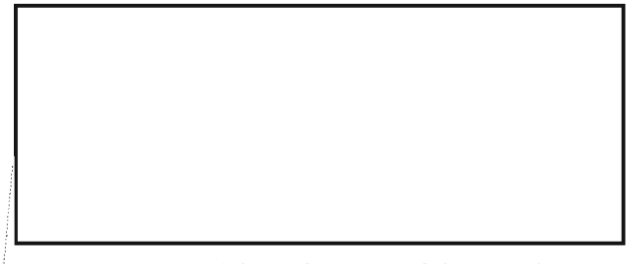
3. Identification and analysis of vulnerabilities

It is almost axiomatic that no operation or system can be relied upon to be perfect in this imperfect world. Almost every one possesses certain inherently exploitable conditions, that is, vulnerabilities that could permit an adversary to acquire critical information. Furthermore, at times the adversary can use inherent vulnerabilities to induce still other vulnerabilities in the system. Prominent among vulnerabilities is human frailty. Frequently OPSEC analyses reveal stereotypic procedures or other poor practices that reveal critical information.

Because of the high value of the information that can be derived from exploitation by adversaries, the cryptologic community must be extraordinarily aware of vulnerabilities. For example, some variations of activity at a site may give an insight into its mission when an adversary correlates it with a remote event previously unconnected to the site's role.

4. Risk assessment

In this step an assessment is made of the impact of an adversary's acquisition of critical information, and practical countermeasures to be considered are identified.



An important and difficult aspect of this step is an estimate of the degree to which the additional or changed countermeasures are expected to reduce the risk, and the cost associated with their adoption. In the case of the cryptologic community, the costs of implementing recommendations resulting from OPSEC analysis have almost uniformly been modest relative to the high value of the critical information to be protected.

5. The application of appropriate countermeasures

This, of course, is the payoff. In the OPSEC process, the final determination of what countermeasures to implement is made by the managers of the operation or activity since mission accomplishment and resource management are their responsibility.

OPSEC PLANNING AND SURVEYS

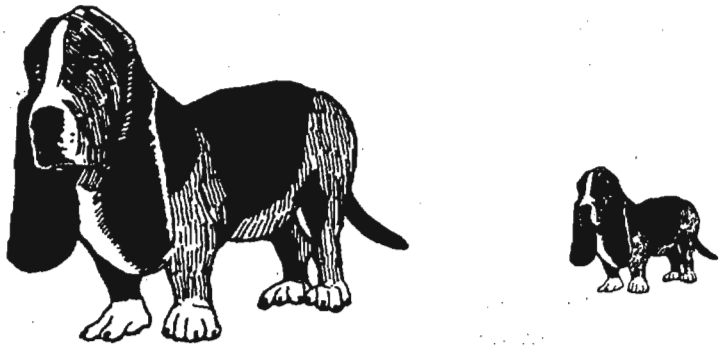
To be most effective, OPSEC planning must be an integral part of operations planning. It is essential that personnel involved in operations planning be versed in OPSEC. Where feasible, it is also very helpful to have operational plans analyzed by an independent, multi-disciplinary OPSEC team. The team should be composed of people fully knowledgeable of the details of the operation, along with specialists from intelligence, security, communications, logistics, ADP support, and so on.

OPSEC surveys using multi-disciplinary teams are an integral part of the overall OPSEC process. In almost all cases the teams can identify critical vulnerabilities that are or would be revealed during actual operations and that are frequently overlooked by personnel involved in routine.

DIRECTIVE 298

In view of the demonstrated value of OPSEC, in January 1988 the President issued National Security Directive 298. This requires all organizations with, or supporting, national security missions to establish formal OPSEC programs, to plan for and implement OPSEC in their agency's activities, and to make sure that all personnel are aware of the threats, and that they understand the OPSEC process.

DEPUTY DAWG



[redacted] P.L. 86-36

How many times have you heard an Agency manager say that he or she enjoyed being the chief of a lower organization more than being the deputy of the next higher level organization? There seems to be more satisfaction to being the Lone Ranger than being Tonto. Yet in this Agency, the deputy position serves a valuable role in meeting both mission requirements and personal career goals.

Being a deputy should provide a good learning and growth opportunity, though it is seldom anyone's final career aspiration. This paper offers some thoughts about the various roles a deputy chief may play.

The deputy position is common in both the civilian and military sides of government. It is generally absent in the private sector. The conventional wisdom is that profit-dependent organizations either cannot afford (or chose not to) the overhead expense inherent in deputies. When the boss is away, someone from the next level may or may not fill in. In one person's words: "When you are the boss, you are always the boss, whether you are on a business trip or a vacation. If there is someone else in your organization who can do your job while you are away, he or she will—and you will be looking for another job."

There is very little in the academic and professional literature on the role of deputies. Perhaps most authors assume that no self-respecting, hard-charging, and upwardly-mobile professional is interested in playing second fiddle. Perhaps it only reflects the general absence of deputies in the private sector. Or perhaps this absence reflects a belief that there is no real need to write specifically about deputies: the literature addresses management concepts, techniques, and ideas that apply to any executive or manager, whether chief or deputy.

Profit-dependent organizations tend not to be as concerned about long-term career paths for their employees. If no one in the organization has the skills required for a particular management or executive position, the company goes out and hires someone who does. Indeed, managers and executives in the private sector often progress along their career paths by moving through a number of companies.

Our unique business demands that we have a stable, experienced, and highly trained workforce. Our policy of promoting from within not only helps us keep a high employee retention rate but also ensures a pool of qualified people

capable of stepping into higher management positions when needed. The deputy position enhances the ability of our system to provide qualified people to move up.

The primary justification for a deputy is work load. When the work load is so great that a chief cannot handle his or her responsibilities without excessive stress, the health of the organization and the individual may suffer.

Another significant reason, which should be related to the first, is to provide a training opportunity. The deputy role permits someone who previously was concerned only with a more narrow perspective to see a larger one. It allows the person to learn how to manage the larger organization and to work in the bigger picture— and do so with less risk to the mission and health of the organization than would otherwise be the case. In meeting these two goals, the position also serves as a testing ground for potential chiefs.

The role any deputy must play depends on the chief's style and wishes. Generally speaking, deputies have to repress their own egos in favor of their chiefs'. Loyalty and patience are required traits. Secure chiefs will not want a mirror image of themselves. The prime responsibility of subordinates is to give the bosses their best professional judgement. This is especially true for a deputy. The value of a deputies may be measured by the work load they can absorb from the chiefs and by the manner in which they complement the skills of the chief. Some of the roles a deputy may play (they are not mutually exclusive) include:

◆ Advisor. All subordinates, especially deputies, owe their supervisors their best professional judgments. This means telling the chief what the deputies believe is right, not just what they thinks the chief wants to hear. This requires a chiefs who are willing to listen to ideas and judgments that may be contrary to their own. The advisors also haveo be mature enough not to sulk or feel threatened when the chiefx do not accept the advice offered.

◆ Assistant. Deputies as assistants help the chiefs in all or most organizational matters. The two truly share the organizational work load, with the chief making the final decisions and signing off on finished products. Sometimes, the chief delegates certain functional areas to the deputy, who then acts as the final authority for the organization.

◆ Team member. The deputy works as an equal partner with the chief, although the chief, as in all cases, retains ultimate responsibility. This may require a chief who is more interested in achieving organizational objectives than worrying about whose idea something was. It also requires a deputy who does not try to upstage the chief, and who is more interested in successfully reaching organizational goals than gaining personal credit.

◆ Back Up. The deputy as back up is one who stays fully informed on the chief's policies, concepts, wishes, etc., but steps in only when the chief is absent.

◆ Project Manager. In the project or task manager mode, the deputy handles only specific projects assigned by the chief. This allows a deputy's special interests or talents to be concentrated on special problems or issues vital to the organization.

◆ Intermediary. In this role, the deputy serves as the communications link between the chief and subordinate supervisors and/or the non-managerial ranks. The deputy may serve as the "people-oriented" member of the management team, while the chief fills the "task manager" role.

◆ Inside Person. In this role, the deputy manages the internal operations of the organization while the chief does the outside political or public relations work.

◆ Student. The deputy position permits the incumbents to improve management skills and increase their expertise in the organization's technical areas of responsibility.

The effectiveness of a deputy may not be easy to measure except in contrast with periods of prolonged absence. The standard of measure-

ment in the absence of a deputy would include the chief's work load growth, the increase of stress, and the organization's efficiency.

Deputies may be most effective when they absorb work load the chiefs do not covet, when they provide skills in which the chief is either lacking or simply does not excel, and when they are able to facilitate communications within the organization. Deputies are also effective when they serve as peer-level sounding boards for management, policy or personnel matters. From a chief's point of view, the effectiveness of a deputy may be measured in the sense of "comfort" the deputy provides to the chief.

Serving as a deputy does offer a number of positives. It offers a chance to contribute to the organization's mission while learning more about the "big" picture. And it allows the deputy to study the chief's managerial style "up close and personal." A deputy can attack organizational problems that otherwise might not come to the attention of the chief, or on which the chief would not have time to focus. And a deputy may be able to propose ideas and solutions to issues that might be overlooked because of operational pressures on subordinates.

There are draw backs too, of course. The primary one is that a deputy's effectiveness and utility is directly dependent on the style of the chief. It is easy for hard-harging deputies to become frustrated. Depending on the style of the chief, authority to act may not be there, and perspectives and ideas may be filtered. Exposure to Agency executives may be diluted, and the ability to directly influence actions may be less than expected.

Deputies serve a valuable role in meeting the challenges this Agency faces, and the position can serve as an important rung up the career ladder. The success of any particular deputy depends, as it does in most things in life, on the incumbent's professional and personal skills, and a degree of good luck. ❑

KRYPTOS

Cryptanalytic Literature Competition

open to all NSA employees

closes COB 30 June 1990

Papers may treat any topic in the broad category of professional cryptanalytic literature, including:

- attacks and techniques relating to cryptanalytic problems
- cryptanalytic research
- history of cryptanalysis
- other subjects relating directly to cryptanalysis, such as target studies, cryptologic trends from the point of view of cryptanalysis, computer support of a cryptanalytic problem.

Papers written between 1 July1989 and 30 June 1990 are eligible. They may be written specifically for the competition.

Entries may carry a classification up to TSC. Compartmented papers will be considered only in extraordinary cases.

Criteria

- Is the paper an original discussion of a cryptanalytic subject?
- Is the paper well written? Is the subject presented well? Can the reader with a suitable technical background but unfamiliar with the subject understand the paper and, by reading it, gain knowledge about the subject?
- Does the paper constitute an important addition to the body of cryptanalytic literature?

To enter, send four copies to :

[redacted] A547, Ops 2A

P.L. 86-36

The following is reprinted, with permission, from R5 Tech Briefs, *July 1989, "Literature Reviews and Recommendations." Written by some of Dave's friends, it is a tribute to a model professional. CRYPTOLOG is proud to have been among the beneficiaries of Dr. Harris's many efforts to inform and inspire.*

David Harris

in memoriam

(b) (6)

(U) David Harris passed away at his home on 14 July 1989 after having served over 10 years with NSA. It is appropriate to write of him here as his contributions carried 99% of this column since this magazine began publication last year. [redacted] His passing will mark a large change in R51's activities and reports, as others try to take up only some of the many things that Dave did so well.

(U) To describe what Dave Harris has meant to R51 and to the National Security Agency, perhaps it is best to begin with a parallel from a novel of Chaim Potok. The conflict in *The Chosen* revolves around whether the main character will take up the career for which he seems to have been chosen by his brilliant intellect, his insight, and his command of an immense body of knowledge. In the case of Dave Harris, we were fortunate that he decided to join our business, rather than pursue an academic career in the field of Algebraic Geometry.

~~(FOUO)~~ Having chosen this alternative career, Dave plunged into the world of cryptomathematics wholeheartedly. In February 1979, he began his career with NSA, entered the class of 1982 P1 Cryptologic Mathematician Program (CMP), and had very productive tours in G95, R14, G42, A54, and S61. Upon graduation from the CMP he joined R51 where his great energy, organization, and breadth of mathematical knowledge made him invaluable. In R51, the office of Mathematical Research, he played increasingly important roles as researcher, teacher, and leader.

(U) In conducting research on a variety of problems, Dave drew not only on his previous broad academic background, but on his great versatility and quick grasp of new fields. He soon became expert in several areas of statistics with applications to our problems, most notably the interplay between moments problems and Pearson curve fitting which is recorded in his article in the *Proceedings of the NSA Mathematical Sciences* Meetings. His intuitive grasp of cryptomathematics is illustrated by the fact that the credit he received for MA-250 came from his teaching the course, despite not having taken it previously himself.

(U) In seminar and informal working discussions, Dave could always be counted on for relevant and perceptive comments and suggestions on how best to attack a problem, or rethink a process in order to extend its generality and applicability. Several of his particularly insightful solutions to statistical consulting problems earned him Letters of Appreciation during his two-year assignment in R513, the Statistical Techniques Division. He was eager to consult and his interest in statistics was also shown by his membership in the American Statistical Association and the Institute of Mathematical Statistics, R513 is deeply appreciate of his work

and interest in NSA statistics during and after his tour there.

(U) Examples of his contacts with outside academia were his survey of work on the Mordell Conjecture which appeared as one of the prestigious expository articles in the Notices of the American Mathematical Society for June 1986, and his correspondence with Professor Nicholas Katz of Princeton University on some deep conjectures concerning Kloosterman sums over finite fields of characteristic two.

(U) As a teacher, with an interest in passing on and fostering knowledge in classified and unclassified mathematics, Dave Harris kept his finger on the pulse of developments in an amazing number of fields, and communicated pertinent summaries through the R51 Seminar, these literature reviews, his famously comprehensive and incisive trip reports (often numbering 5, 10, 15, and even 20 pages in length), as well as individual research papers. During his record-breaking term (over five years) as coordinator of the R51 Seminar, Dave molded it into an institution with his own personal stamp. The R51 Seminar was carefully planned to continually survey the major new developments in all corners of NSA, and was, incidentally, an area where his skill with words and love of puns were strongly displayed. The speakers usually found that the most perceptive questions and observations came from Dave himself, as he would "do his homework" by reviewing the speaker's previous work on the subject before attending a presentation.

(U) The literature reviews need only be mentioned to our readers to recall the breadth of coverage, personal insight, and craftmanship of composition displayed every month. Similarly, his coverage of a Mathematical or Computer Science conference was unequalled, from his advance planning and surveys of talks for coverage, through his careful note-taking at as many talks as he could possibly attend at any conference or seminar, and his very detailed reports. In his individual research papers on classified topics, he took up themes of interest for their applicability, while a natural instinct for teaching led him to keep a supply of problems

An excerpt from his contribution to the publication commemorating his 25th Harvard class reunion:

I have been reasonably happy with my job. It allows me to dabble in whatever subject comes to hand . . . I still consider myself a mathematician. Recently I have been trying out the high-prestige career of Defense Department manager. I try to serve others, and help them do whatever they do well . . .

I would like to advertise President Bok's by-now-forgotten speech at the 1988 commencement. He dealt in part with the problems of preserving a government competent to handle the tasks we assign it. When people run down government employees, they discourage capable people from getting involved. If you believe our present system inadequate to handle the problems facing it, or that it is going the wrong way from time to time, do not stay safely on the sidelines telling us that we cannot do the job. You are right. I will probably fail to make any difference. The politicians of both parties do not help. But I do try my best to move things in what I think is the right direction.

In the present world of scarce resources for government, math and science are competing with housing for the poor. How shall we juggle priorities in this situation? Whatever you and I think, these needs are not likely to be met by cutting the national defense whenever money is needed. Math and science cannot afford to be parochial in assuming themselves the highest public good. And the pragmatists and humanitarians cannot ignore the need to arrange for the future. A proper balance between the long and short term, pure and applied, pragmatic and humanitarian, must be sought. It is important that these decisions not be made in the typical way —in accordance with the relative strengths of the lobbies involved, each acting in its narrowly conceived self-interest. Those willing to try to strike the balance on broader grounds must be discouraged. Currently, the American system in government and industry acts to encourage managers to consider only payoffs that will become apparent during their own brief tenures in office.

UNCLASSIFIED

suitable for those just beginning to study crypto-mathematics.

(U) During 1988 and 1989, Dave took a turn as Division Chief of R512, the Consulting Division within R51. Here his sense of personal responsibility and integrity contributed to a selfless period of service to his fellow researchers and to the future good of our organization. He functioned alternately as cheerleader, planner, and advocate of his employees. He sought to provide a dialogue on organizational goals, on technical ideas, on what role management played in R51. And in keeping with a typical Dave Harris style, he produced toward the end of his term of office a closely-spaced, tersely written 4 1/2 -page set of informal notes: "Survey of the Job of an R51 Division Chief." He planned thoroughly for his meetings with management, tried his level best to advance the concerns of those beneath him, and generally took on the role of a caring and concerned parent.

(U) In his building of mathematics within R51 in his "alternative career" as researcher, teacher, and leader, one fact about Dave Harris especially struck those of us privileged to work with him: he was a thoroughly good man. He put the good of others before his own, the growth of knowledge before personal advancement, and was truly the "righteous man" spoken of in Chapter 18 of Genesis.

P.L. 86-36

Editor's Note:

Just a small fraction of Dave's many reviews and reports that appeared in R51's Monthly Research Summary have been republished in CRYPTOLOG. There still remains a considerable backlog on which we will continue to draw from time to time. A sample appears on page 24 of this issue. Dave was most gracious in giving CRYPTOLOG carte blanche on publishing his writing.

BULLETIN BOARD

CQ UNDER NEW ORGANIZATION

(U) *The Cryptologic Quarterly*, NSA's professional journal, is now published under the auspices of a new organization, D9, the Center for Cryptologic History. The Chief is David Gaddy, OPS 2B, 963-1891. Submissions to CQ should be sent directly to the Managing Editor, [redacted] D91, SAB 2 Door 22, 972-2235.

FOR TRAFFIC ANALYSTS

[redacted]

CA SOFTWARE RUNNING ON UNIX

~~(FOUO)~~ CRYSCOM has initiated an exchange program for CA software running on UNIX contributed by various CA organizations. Available are complete packages, individual programs, and subroutines. For a complete list please get in touch with [redacted] CRYSCOM Exec, P13, 963-3045, or [redacted] CRYSCOM Chairman, P1/A548, 963-1464, or one of the following points of contact: J.

[redacted]

~~FOR OFFICIAL USE ONLY~~

The Mysteries of ΓAMMA

Γ,γ γάμμα, τὸ τρίτον γράμμα τοῦ ἑλλην. ἀλφαβήτου, δεύτερον σύμφωνον· ὡς ἀριθμητ. σύμβολον γ′=3 ἢ τρίτος καὶ ,γ=3000.

Richard D. Sylvester, B

~~(S-CCO)~~ Many people who have been granted GAMMA access have only a vague understanding of what this special access is, or they have no idea at all what it constitutes. GAMMA is an unclassified coverterm used to flag especially sensitive Category III COMINT product. The term signifies that the product requires maximum security protection for one or more of the following reasons:

[redacted]

~~(C)~~ Although the term GAMMA used alone is unclassified, the fact that the term is related to COMINT is classified, at a minimum, CONFIDENTIAL. In addition, information which has been reported in GAMMA product reports may not be referenced in non-GAMMA product nor revealed to personnel not cleared for GAMMA access.

~~(C)~~ DDO is the authority responsible for identifying that COMINT which is to be handled in GAMMA product reporting channels. Proposals for assignment of sensitive COMINT to the GAMMA series are made to DIRNSA, through the GAMMA Control Officer, for DDO approval. NSA keeps the National Foreign Intelligence Board (NFIB) informed of the nature of the information placed in this series and justifies each assignment in such detail as to convey the security risk inherent in dissemination of the information.

~~(FOUO)~~ The dissemination of GAMMA reports is tightly controlled. To assure proper handling of GAMMA information, the DDO nominates and DIRNSA appoints a GAMMA Control Officer (GCO), who is responsible for all aspects of the handling and distribution of GAMMA material and maintaining records of that SIGINT which requires GAMMA protection. [redacted]

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

[redacted]

~~(FOUO)~~ For additional classification guidance concerning the GAMMA control system, contact the the appropriate person at your Division, Office or Group level, or the GCO in P0522, or refer to

[redacted]

P.L. 86-36

[redacted] G96 P.L. 86-36

Thoughts on

ORDERING, SORTING, and HEAPING on CRAY

I was pleased to read [redacted] years I have know [redacted] to be one of the best sorting packages available. Now, however, I find that some of the others (which I thought to be efficient) are not so hot.

P.L. 86-36

Many of the "good" routines are merely drivers for [redacted] No doubt, the sort algorithm(s) used by [redacted] should and will have a major influence on future sorting, ordering and (possibly) heaping routines.

Algorithms to save the top-n best answers (which I'll group under "heaping") are related to, but should be considered separately from sorting and ordering. When heaping, we have a large degree of control concerning the format of the heap - that is, the heap is already ordered (in some way) when the next answer is about to be inserted. Heaping requires that the heap be continually updated as new (best) answers are produced.

Sorting and ordering require less interaction with calling programs, and the algorithms used can dynamically allocate and release space as needed. (Heaping requires dedicated space for the duration of the heap.)

[redacted]

P.L. 86-36

GENERAL COMMENTS

What commercial routines are available? Or ones from academia? P.L. 86-36

While conversion from [redacted] to UNIX is a tremendous burden, it is also an opportunity to review, revise and consolidate major processes. Ordering/sorting/heaping is one of the topics which deserves and requires a great deal of attention, since applications of such routines are so pervasive.

Technical Literature Report

Reported by: David Harris (see page 18)

(U) S. Radziszowski & D. Kreher (1988) "Solving Subset Sum Problems with the L^3 Algorithm," *Journal Combinatorial Mathematics and Computing*, 3, April 1988, pp. 49-63.

~~(C)~~ The authors are interested in what most people call the knapsack problem, and in particular with speeding up attacks on it using the lattice basis reduction algorithm. They reduce the number of multiprecision operations needed. The authors also use a direct search for short vectors to complement L^3. The authors claim the run time is an order of magnitude better than that of Lagarias and Odlyzko, and that as a result higher density subset sum problems can be solved. While there is no proof the new algorithm beats its competitors, there are practical examples that this is true. The authors give some ideas for further improvement.

(U) Daniel Fuhrmann (1988) "An Algorithm for Subspace Computation, with Application in Signal Processing," *SIAM J. Matrix Anal. Appl.*, 9 (2), April 1988, pp. 213-220.

~~(C)~~ There are many situations that involve using eigenvectors, eigenvalues, or singular values to recover information hidden in a matrix. An algorithm for computing the eigenvectors corresponding to the m algebraically smallest or largest eigenvalues of an nxn symmetric matrix A is given, where m is small compared to n. In addition to cryptanalytic applications, such methods come up in signals processing as in the MUSIC algorithm for bearing estimation. When n is large and A is structured, the Lanczos method and its variants are best.

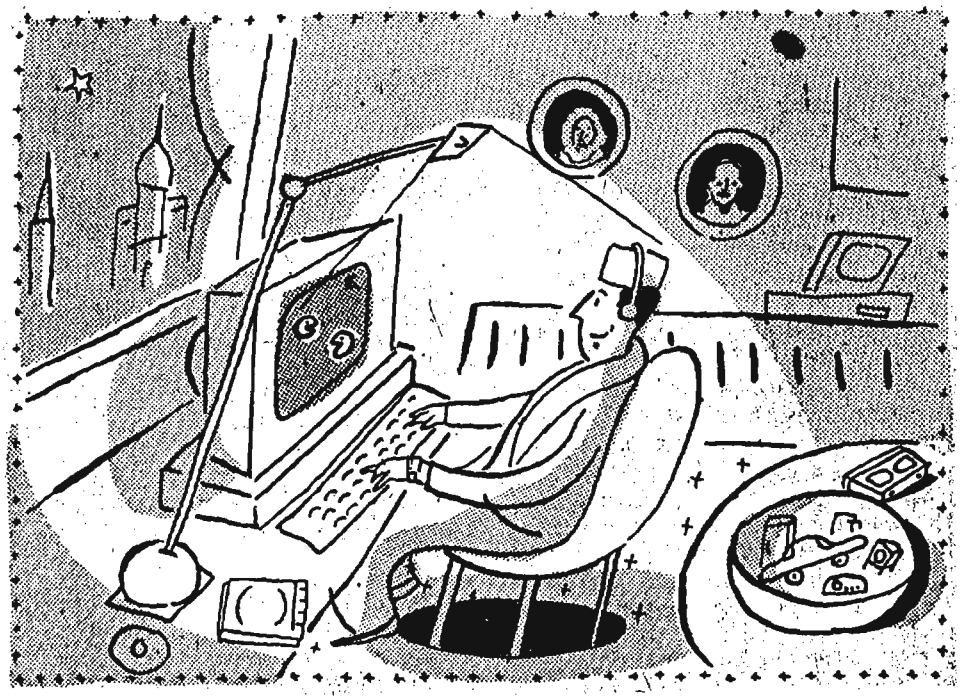
~~(C)~~ This paper proposes a Lanczos-like algorithm consisting of repeated applications of the Rayleigh-Ritz (RR) procedure to a sequence of subspaces which converges to the desired invariant subspace. The RR portion of the algorithm is highly structured din a way that the author hopes will lead to significant computational savings at little cost in memory. All the computations lend themselves to parallel implementation. The author's goal is "an adaptive formulation of Schmidt's MUSIC algorithm, or alternatively, an adaptive eigenvector beamformer, in which the weight vector for an array of antennas or sensors is determined from the eigendecomposition of the received signal covariance matrix."

(U) Robert M. Kuhn (1988) "Curves of Genus 2 with Split Jacobian," *Trans. AMS*, May 1988, **307** (1), pp. 41-49.

~~(C)~~ An algebraic curve has a split jacobian if its jacobian is isogenous to a product of elliptic curves. Given a curve X of genus 2, and a map from X to an elliptic curve E, then X has a split jacobian, but the complement to E in the jacobian of X is not uniquely determined. However, under certain conditions, there is a canonical choice of the complementary curve E′ and the map from X to E′. Kuhn shows this, and gives an algorithm for finding that curve. The construction works in any characteristic *other than 2*. Applications are given in characteristics 0 and 3.

~~(C-CCO)~~ In theory, the analysis of such splittings is relevant to solving the discrete logarithm problem on the jacobian (a Harris upgrade of a suggestion of Mike Paul.) The degree of the isogeny is crucial to any crypto application, and turns out to be the size of the kernel of the direct sum of two maps. The jacobian of dimension 2 is the next step up from elliptic curve discrete log problems. Of course it is not clear this will ever be of practical importance. Split jacobians are used in the theory of abelian varieties to construct counterexamples, and families of curves with maximal numbers of points in finite fields. The study of coverings of curves by curves is at the heart of the paper. □

Review



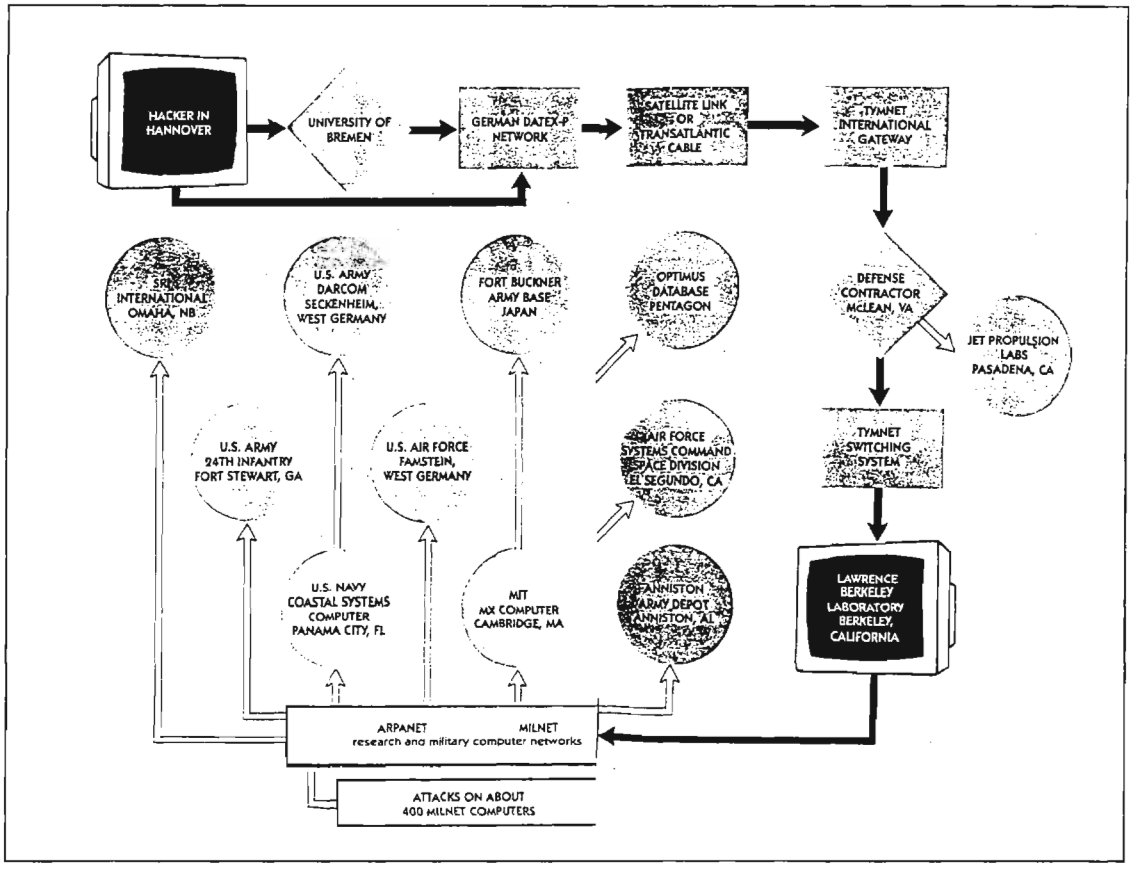
The Cuckoo's Nest
by Cliff Stoll. Doubleday, New York, 1989

P.L. 86-36 *Reviewed by:* [redacted] *P13*

(U) A German computer hacker penetrated a computer at Lawrence Berkeley Laboratories (LBL) in August 1986. This caused a 75-cent discrepancy in the system accounts. Clifford Stoll, an astrophysicist who had run out of grant money, was given a job at LBL computer center, and as the newest programmer was asked to check the discrepancy. Thus began a frustrating and fascinating international hunt that lasted for a year, finally leading to conclusive evidence of a KGB link to a ring of German Hackers.

(U) In *The Cuckoo's Egg*, Stoll has written an intriguing and suspenseful tale of computer sleuthing, bureaucratic muddle and indifference, and the exploits of a cunning hacker, counterpointed by the tenacious struggle by a single concerned scientist determined to find the unknown hacker. One of the ironies revealed by the book is that the thicket of laws and administrative restrictions established to protect the privacy of communications in fact make it almost impossible for computer managers, telecommunications operators or Government agencies to detect or pursue hackers who penetrate computers and E-Mail systems. Unchecked, the penetrators can read or alter anything they want within the computers.

(U) When Stoll began to investigate the 75-cent discrepancy, he found an unregistered user



"Hunter" had been using the LBL computer. One day later an E-Mail complaint arrived claiming that some LBL Unix user had tried to penetrate a DOCKMASTER computer in Maryland. Checking showed that only one LBL Unix user Sventek was logged in, but he was in England, with no access to the computer. There was no clear proof of a hacker, just circumstantial evidence. Stoll's superior was unimpressed, and demanded proof. Stoll began to secretly monitor who was using the Unix system, and soon saw a log-in by Sventek. Stoll traced the port. By chance, a hardware technician who knew the computer center communications complex had been collecting statistics on who had been using the communications switchyard. This showed a 1200-baud connection, which meant an outside phone line. The discovery narrowed the search to about 50 phone lines. So Stoll decided to tap the 50 phone lines and printout the modem traffic — so that the hacker could not detect, from *inside* the computer, that the E-Mail was being intercepted. Stoll's girlfriend, a law student, assured him that since he was not the Government, he didn't need a warrant (p,.20). With a clear conscience, Stoll borrowed 50 printers, teletypes and portable computers on a Friday night in September, and printed out all the E-Mail traffic, keystroke by keystroke. One of the printers had 80 feet of printout, and evidence of how the hacker operated.

(U) The transaction, sent through Tymnet, showed that the hacker had been on the machine for three hours and used a special editing program called Gnu-Emacs which allowed him to bypass the Unix controls to change a Unix program ATRUN. The hacker then used the changed Unix operating system to make himself a privileged user. The original ATRUN program was replaced and all trace of the transaction erased. This was like a cuckoo bird laying its egg in another bird's nest, to let the victim hatch the cuckoo's egg. Once the hacker became a privileged user, he could bypass all the privacy protection in the computer. Without the warrantless wiretaps, this penetration would have

been undetectable, for the hacker's penetration program was watching for *internal* surveillance.

(U) In time, Stoll set up an interception system that not only spotted and recorded the hacker's transactions, but signalled him in morse code on his telephone beeper, so he would know instantly, day or night, when the hacker was on the line.

(U) The hacker was not content just to penetrate into the LBL computer, but got into university and government computers all over the US and abroad. Usually the system managers had no hint of any trouble until Stoll, reading his intercepts, called them and told them what to check for. Without the year-long accumulation of intercepts, the extent, modus operandi and source of the hacking could never have been determined.

(U) In due course, Stoll and LBL contacted the police, the FBI, NSA, CIA, AFOSI, Tymnet and the German Bundespost. The carriers, Tymnet and Bundespost, were very interested, and energetically traced calls whenever Stoll's pager signalled him. Eventually this found the hacker, who had started working for the KGB after he was able to copy sensitive unclassified military files. But for most of the complex network investigation, the FBI was uninterested because there was nothing they could prosecute; the National Computer Security Center at NSA considered domestic monitoring as "prison term stuff" and stated, "We're here to make computers more secure, not to catch criminals."

(U) In spite of the caveats, CIA, NSA, FBI, DOE and the Pentagon *did* in fact keep up with the case, asked Stoll for copies of his intercepts, and invited him to tell his story to very high level audiences. The Defense Department sealed up its computers to prevent penetration. But what the agencies could *not* do was intercept, trace or pursue the hacker.

(U) Stalled by the C&P telephone company who would not tell him where the hacker was getting into Tymnet, Stoll finessed the long distance operator into revealing enough information to track the connection back into Mitre corporation in Maclean, VA. Further work showed that the hacker was getting across the ocean into Mitre, and making Mitre pay the phone bill for both the incoming transatlantic calls from Germany, and numerous outgoing calls around the US. Mitre refused to believe that was possible.

(U) Stoll set up a "sting" operation with counterfeited classified documents. Government interest vacillated. Stoll was told repeatedly he had "only one more week" to catch the hacker. The FBI closed the case. Stoll discovered the hacker had passwords to a number of systems, and knowing from his intercepts that the hacker had been stealing *encrypted* passwords, deduced that the hacker used the published encryption algorithm to encipher dictionary words until he got matches with the encrypted password files!

~~(FOUO)~~ Then in April 1987, a letter from Pittsburgh (p.64) in response to the sting enabled FBI counter intelligence to show a KGB link via the Bulgarian secret service. This revived official interest, and exposed a team of German hackers selling Unix operating software copied from US military computers and some passwords into military files, to the KGB. This led to a prosecution in Germany which concluded in 1990 with the hackers convicted and set free, because, under German law, they had not caused serious harm to West Germany (Reuters 15 Feb 90). Another point in the German case was that Stoll's intercepts could not prove that it was the *same* individual who was penetrating into the LBL computer (ibid.). That bizarre legal outcome was typical of the mismatch between the law and the actions and effects of the hacker.

~~(FOUO)~~ The book, which has become a best seller, draws a rather unflattering portrait of interagency buck passing and turf battles. Stoll tracked the hacker down, despite all of the resistance and indifference, because he got involved , and because he had enough freedom to pursue the trail where it led by any means he could devise. In his quest he pioneered in a number of techniques of "network investigation," useful tools in computer security.

~~(FOUO)~~ This raises an interesting point about privacy laws. Stoll's initial intercept of 50 phone lines was done, without a warrant, in early September 1986, when there were still no legal restrictions on intercepting data traffic on telephone lines. The local phone company would not trace the hacker's calls *without* a warrant, even though a warrant was *not* required. However, Stoll continued to monitor all the traffic over four telephone lines connected to Tymnet and sent printouts of the intercepts and logs to various government agencies. Without the intercepts and logs the search would never have led back to the hacker and to the KGB.

(U) PL-99-508, which changed the interception law, went into effect on 21 Oct 1986. The law, codified in 18 USC 2510-11, does not authorize computer managers to monitor content of electronic communications. New laws concerning computer networks in 18 USC 2701-2 came into effect only at the end of 1988, and they also do not authorize intentional wiretapping, nor do they authorize disclosure of deliberate interceptions to a law enforcement agency (18 USC 2702(b)(6)).

(U) What Stoll's book illustrates, in spellbinding detail, is that purely passive measures of defending complex modern networks against skillful attack are inadequate. Without *network investigation* techniques, i.e. domestic interception, records keeping, and general search over suspect channels (Stoll searched 50 lines!), it is impossible to get enough information to detect even very serious threats to security and privacy.

~~(FOUO)~~ Law enforcement agencies cannot get warrants for general search, and they usually cannot tell *who* is hacking or *which circuit* will be used. Those specific data are required for interception warrants (18 USC 2518(4)). The carriers can check every voice circuit they operate, but *not* for content (18 USC 2511(2)). There is no authority for carriers to monitor non-voice traffic. The authority of computer center operators to intercept the *content* of all the communications in and out of their computer complexes is not clear, for it depends on whether the system operator is considered a *party* to the communication (18 USC 2511(2)(d)). Usually the system operator is not a party to the E-Mail communications, just as a PBX operator is not a party to voice communications. Government agencies are not allowed to obtain or use the contents of intercepts unless they satisfy the interception laws (18 USC 2511(1)(d)). *All* LBL computer users coming in through the Tymnet lines were intercepted, even though they were not engaged in any wrongdoing, and had a right to all the privacy the law provided. The Hanover hacker was deliberately trying to *avoid* the system operator, because he did *not* want the system operator to be a party to the transaction.

(U) The new laws permitting certain disclosures of information stored in computers apply only to organizations "providing remote computing services to the *public*" (18 USC 2702(a)(2). Since most computer networks require password access, they are *not* available to the general public, in which case the operators apparently have no legal authority to disclose information, even if it was inadvertently obtained. There is a private organization CERT (Computer Emergency Response Team) at Carnegie-Mellon University, chartered by DOE to respond to hacking, viruses, etc., but its authority to do anything but advise is very unclear. It is also not clear that US privacy laws or computer crime laws can be applied to a person outside the US — the Germans applied only their own laws to the German hackers. Finally, as the German courts pointed out, no one could prove that it was the same person on every call, or that he was causing any specific harm.

(U) Thus, in a beautiful paradox, the laws set up to protect the privacy of citizens against government surveillance ironically shield the activities of hackers or malicious penetrators from any surveillance, so they can tamper and exploit the files and communications of legitimate E-Mail and computer users, leaving them as defenseless as an unknowing cuckold. ❐

Review

Reflections on Intelligence by R.V. Jones. 376 pp. Heinemann: London, (1989)

Reviewed by: Vera Filby, E4

Among the procession of now-it-can-be-told books on the history of World War II published in recent years, one has stood apart from the rest for its focus on the scientific and technological aspects of the war and its view of events from the highest levels of science and government. In *Most Secret War*, R. V. Jones, now Professor Emeritus of Natural Philosophy of the University of Aberdeen, recorded the struggles and achievements of military science and technology in Britain and his role as scientific adviser to Prime Minister Churchill. (Jones was the man responsible for breaking Germany's new navigational beacon system, which could direct Luftwaffe bombers with devastating accuracy. His special work with radar was instrumental in the successes of the Allied bomber offensive and the preparation for D-Day.)

The present book is a history and appreciation of scientific intelligence and activities related to intelligence from the prospective of half a century's involvement in the field. The main body of the book, Part One, addresses the philosophy and ethics of intelli,gence and the activities of security and deception. This is supplemented in Part Two by "postscripts" to the earlier work and in Part Three by the solution to the mystery of the Oslo Report.

Professor Jones began his postwar intelligence career in 1952, when Churchill asked him to leave teaching in Aberdeen and become his Director of Intelligence. Less than two years later, having observed and evaluated all aspects of the intelligence scene and completed a report, he resigned and returned to his students. Contributing to his decision was his dissatisfaction with the treatment of atomic energy as something apart from other intelligence and his objection to the assignment of ELINT to GCHQ, which he believed to lack the expertise to deal with it.

Under the heading of intelligence ethics, the author discusses respect for allies, diplomatic bags, covert action, assassination, privacy, and other facets of intelligence, all of which encompass irreconcilable contradictions. These short essays, in a style characteristic throughout the book, combine instruction, commentary, conclusions, reminiscences, and lots of anecdotes and good stories. Some of the stories are old but they are retold here by a master, often with new insights and always with sparkle.

Official secrecy requires a chapter of its own, which begins with the observation that the balance between too much and too little has been pondered at least as far back as Francis Bacon. The author relates with undiminished indignation his own run-ins with security in connection with official suppression of information already released to the public. On a different note, he recognizes the marvel of the silence faithfully maintained for 30 years by thousands of people to protect wartime cryptologic security. He attributes this in part to the system of security developed by the British and adopted also by the Americans, and in part to the loyalty that all felt to others who had participated in the great effort.

But the best and most secure system cannot protect against leaks, disclosures, and indiscretions by those outside its authority. Such violations may be committed because of carelessness, indifference to security, arrogance, or for personal advantage or political motives, or for some combination of reasons. A classic case of political motivation occurred in the 1930s, when Prime Minister Baldwin exposed

the content of Soviet decrypts, resulting in the loss of the source.

Politics can also have the opposite effect - the suppression of information that ought to be made known. Here again Baldwin provides an example by his withholding of evidence of German rearmament on the grounds that the public might be so upset as to cause the loss of the election.

In discussing insecurities nearer to the present, Professor Jones mentions self-importance as a possible factor and cites damaging comments by politicians during the Falklands crisis.

Subsequent chapters explore the interrelationships of intelligence and security, intelligence and deception, and intelligence and command. Each could serve as a textbook on the subject.

The book changes course at this point and turns back to the beginnings of modern military science and technology. Here the author presents a history of World War I weaponry and military science and in doing so pays tribute to to the scientists and inventors whose work was so largely responsible for winning both wars. Subjects covered include radio, sonar, chemical warfare, air warfare, infrared, atmospheric research, and several others. Radio was already well established and had been used in the field during the Boer War; but World War I inspired a great expansion in its development. Along with it, cryptology flourished and brought forth its miracles, only to be dismissed and neglected after the war until it was urgently needed for the next one.

While some scientists were creating the weapons of war, others were applying scientific methods and mathematical analysis to military operations, both tactical and strategic. The author credits the invention of operational science to Benjamin Franklin, recounting a story about Franklin's mock estimate of the cost per head of killing Yankees. This introduces stories of extraordinary men and their accomplishments. Told in Professor Jones' vivid and witty style, they make most entertaining reading. Not surprisingly, the scientists' new and unorthodox ideas were not always welcomed in military circles. But lessons were learned, and as World War II progressed, operational research groups were established in various commands to provide analysis, assessment, and advice.

The rise in the power of scientists and their influence with national leaders brought problems of conflict, responsibility, and conscience. Professor Jones comments on these concerns and the crises of conscience that the uses of science in war, particularly nuclear energy, have caused, and concludes: "Never-the-less, I think that in general scientists need to take the risk of bringing political leaders into their confidence, and that reciprocally scientists have a special claim to be consulted about the exploitation of their ideas. If, as in the case of nuclear weapons, these ideas offer horrifying prospects, it is better in the long run that national leaders and populations generally should be soberly aware of them."

Part Two is a mixed collection of short pieces which supplement or complete stories left unfinished in *Most Secret War*. Responses to that book brought an abundance of new contacts, information, and insights. Official documents declassified and released after its publication revealed or made usable still more material. As his first postscript, Professor Jones recalls the Polish cryptanalysts who escaped after the German occupation of Poland and succeeded despite great difficulty and danger in getting their knowledge of the Enigma machine through to the French. Stories follow about members of the resistance movements and other wartime friends and colleagues, Churchill and other national and military leaders, and former German enemies. There are episodes of risk and sacrifice, missions lost and missions accomplished, intelligence efforts - Peenemunde, for example - revisited. Along with these are accounts of the author's adventures and happenings as he followed up the leads generated by his book. NSA readers will enjoy the story of his visit to Electronic Security Command Headquarters and a slew of other U.S.military, research, and industrial establishments, including NSA. Professor Jones had a very good time.

The document called the Oslo Report was sent anonymously by mail to the British Embassy in Oslo in November 1939 and forwarded to London by the Naval Attache.It has been a center of controversy ever since. It consisted of seven typescript pages and a sealed package. The papers contained information on a German glider bomb, torpedo fuses, radar, and other

weapons and devices; in the box was a trigger part.This unexplained gift was regarded with suspicion by almost everyone who knew about it except Jones, who believed in it and used it to guide him in his assessments of future German developments. It proved reliable time after time, and on one inspired occasion a reference in it was combined with an ULTRA decrypt to reveal that a distance-measuring beam had been added to the German bomber beam-guidance system.

Professor Jones describes in considerable detail the strenuous but fruitless efforts of many searchers, including investigative journalists, to identify the unknown source and in even more detail his own wide-ranging and finally serendipitous efforts. In 1954 he learned the identity of the author and knew that he was a noted German scientist and mathematician, an expert in electronics. At last, in 1955 at a conference in Munich, Professor Jones met Professor Hans Ferdinand Mayer of the electrical firm of Siemens & Halske. He did not tell this story in *Most Secret War* for reasons of privacy and a continuing requirement for security.

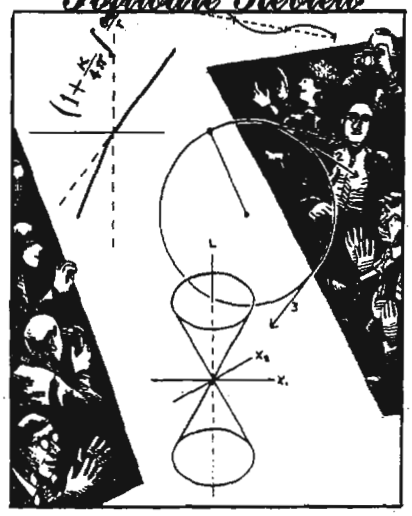
Hans Meyer had been with Siemens for many years and was on a business trip for the firm in Oslo in November 1939. By that time, he had become increasingly disturbed by the evils of the Nazi regime; but he continued with his work in Germany until in 1943 he was reported for listening to the BBC and arrested by theGestapo. He survived Dachau and other camps, escaping finally as Germany was collapsing. He was certified as a victim of fascism by the Allied military authorities and soon went to the United States where during 1946-50 he was a research professor at Cornell working on radioastronomy. He then returned to Germany and Siemens.

This book in its variety -- history, science, studies in intelligence, people and places -- is hard to categorize; but it is easy to recommend for both enlightenment and entertainment.

End Note

Most Secret War. By R. V .Jones. Hamish Hamilton, London. (1978). Published in the United States as *The Wizard War,* Coward, McCall & Geoghegan, Inc. (1978).

Software Review



MATHEMATICA. Wolfram Research, Champaign, IL

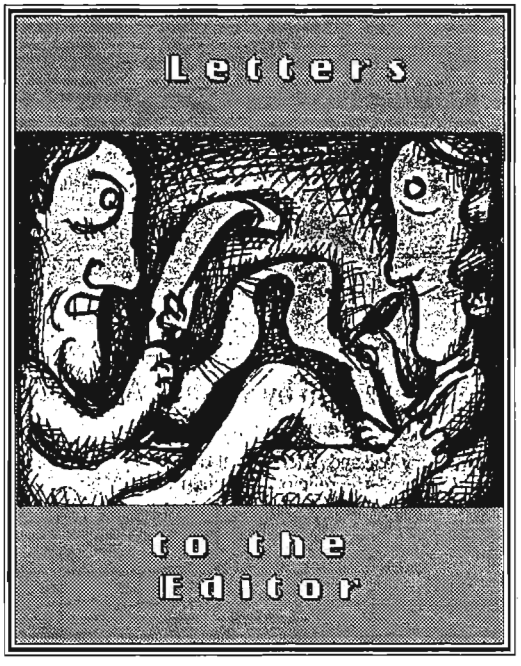
P.L. 86-36

Reviewed by: [redacted] *R562*

~~(FOUO)~~ The symbolic mathematics language Mathematica has been used in two problems [redacted] One is constructing a primitive irreducible polynomial of degree 256 over GF(2), namely, $x^{256} + x^{10} + x^5 + x^2 + 1$. It is known that there are no such polynomials with two, three, or four terms, and this one is the lexicographically least with five terms.

P.L. 86-36

~~(FOUO)~~ The other problem is explicit construction of the Hilbert Class Field of the algebraic number field $Q(\sqrt{-95})$. This was done by closely approximating a root of the so-called Watson polynomial by means of complex Fourier series, then finding the Watson polynomial of degree 8 by using integer lattice basis reduction. All eight roots of this polynomial were then found to extremely high accuracy, and the roots of the class equation computed from them. The class equation itself was then computed as a product of linear factors, and the resulting coefficients rounded to the nearest integer. A positive check was successfully made by factoring both the constant term and the discriminant of the class equation, and finding that the prime factors satisfied a famous theorem of Gross and Zagier. This particular class of equation had already been computed, so we recomputed it with Mathematica as a test, and found that it could do this computation very easily.



To the Editor:

Further to the exchange between [redacted] concerning the use of the term "bastardized" to describe the development of Afrikaans.

I would agree with [redacted] comments on the development of Afrikaans and with his point that the term "bastardized" is derogatory and linguistically meaningless. I feel I can lay claim to some expertise in this matter, as my MA thesis dealt with the various theories about the origin and development of Afrikaans..

[redacted] argues in her response to [redacted] that "bastardization" is frequently used in a technical sense to describe the development of Afrikaans. We are assured that the term is not perjorative. I cannot recall, however, any serious linguistic work I encountered during two years of research into the question that referred to "bastardization" in connection with Afrikaans. The term used by most scholars to describe the development of Afrikaans is "creolization," although there is some question as to whether or not Afrikaans is a true creole. It seems unlikely in the few years since I finished graduate school, a perjorative like "bastardized" could have gained currency in the rather small group of scholars who concern themselves with the history of Afrikaans. P.L. 86-36

[redacted]

Former member, Afrikaans PQE Committee

To the Editor:

I have just seen a bulletin from the National Cryptologic School which is inviting applications for a two-year program designed "to train highly motivated Agency personnel to become the skilled technical leaders for tomorrow's Agency workforce." As a CY-100 graduate, I feel honor-bound to warn potential applicants that this is an empty promise.

When we entered CY-100 in 1968, we were told the same thing about our one-year program: we were to become the technical leaders of tomorrow. When my class compared notes at our twenty-year anniversary luncheon, we found that no one considered CY-100 to have enhanced his or her career; if we are the technical leaders of NSA today, why isn't anyone following us?

The bulletin would have you believe that NSA has a need for multi-disciplined analysts. I agree that we do have such a need, but try to find a job announcement that says that. I believed the propaganda: I took CY-100 and went to a great deal of effort to diversify (I am certified as a professional in five technical fields); I know of no one in NSA who has any interest in my diversification.

If NSA management actually believes there is a need for diversification, they should identify some jobs that demand multi-disciplined analysts (such analysts are readily available); and they should enhance the careers of multi-skilled people to demonstrate that such broadening is actually valued.

If NSA management does not believe there is a need for diversification, they should stop telling lies to naive young employees.

[redacted] *P13*

P.L. 86-36

P.L. 86-36

P.L. 86-36

~~SECRET~~

To the Editor:

(U) I read with some misgivings [redacted] praise of W Group ("Cogitations of a Contumacious Cabalist" *CRYPTOLOG*, 3rd Issue 1989), and feel that a molifying response may be in order. I laud [redacted] obvious pride in belonging to the W Organization; however, I found her point to be somewhat obscured and diffused by it. If she is dismayed by what she perceives is a lack of appreciation of W Group by the rest of DDO, then she may be assured that this is by no means the case. On the other hand, if she is trumpeting the unique qualities of W Group and its personnel, it may be best to remember that we are all team players whose efforts should be put in the larger context of contributing to national intelligence objectives. DDO would be truly hampered, but certainly would not "crumble like a house of cards" without W Group.

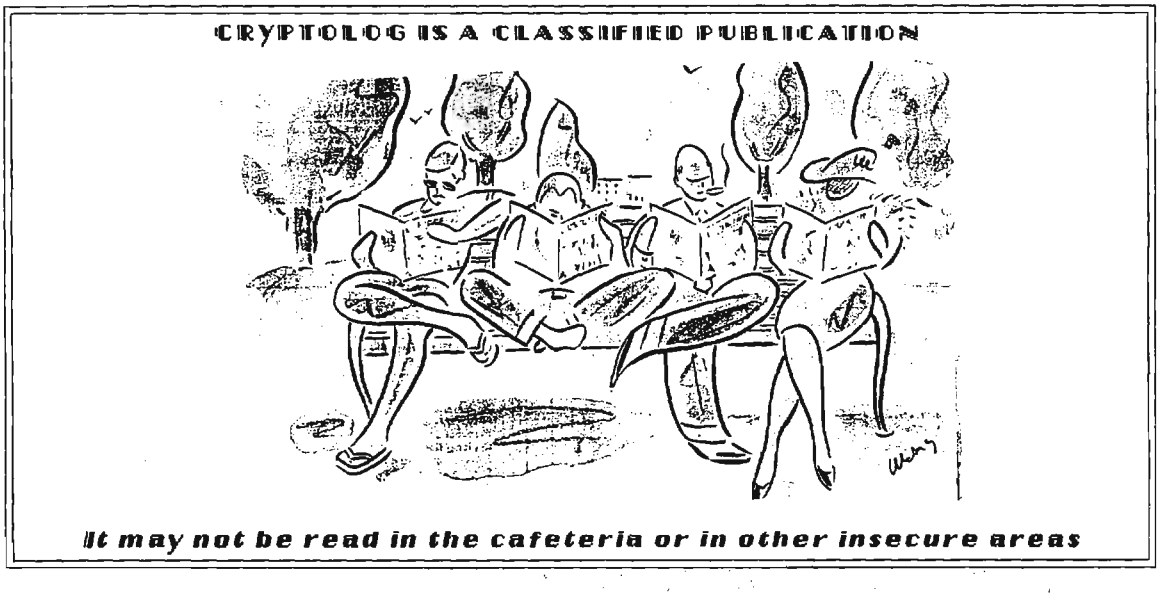
P.L. 86-36

~~(S)~~ It may also have served her purposes better if [redacted] continued her familial symbolism by describing ELINT's split personality - "op" and "tech". Most line analysts should have a passing familiarity with tech ELINT but, if they are involved in military (the current and antici pated de-emphasizing notwithstanding) civil air, telecommunications and tech transfer, or many other problems, Op ELINT is a very important part of their lives. We in B51 have a deep and unabashed respect for Op ELINT. My first introduction to the practical applications of this discipline was in April 1972, and it left a lasting impression on me. That Op ELINT could geolocate, corroborate and and identify individual Vietnamese surface-to-air missile sites, with the result affecting the life expectancy of U.S. air crews, is a lesson I hope never to forget.

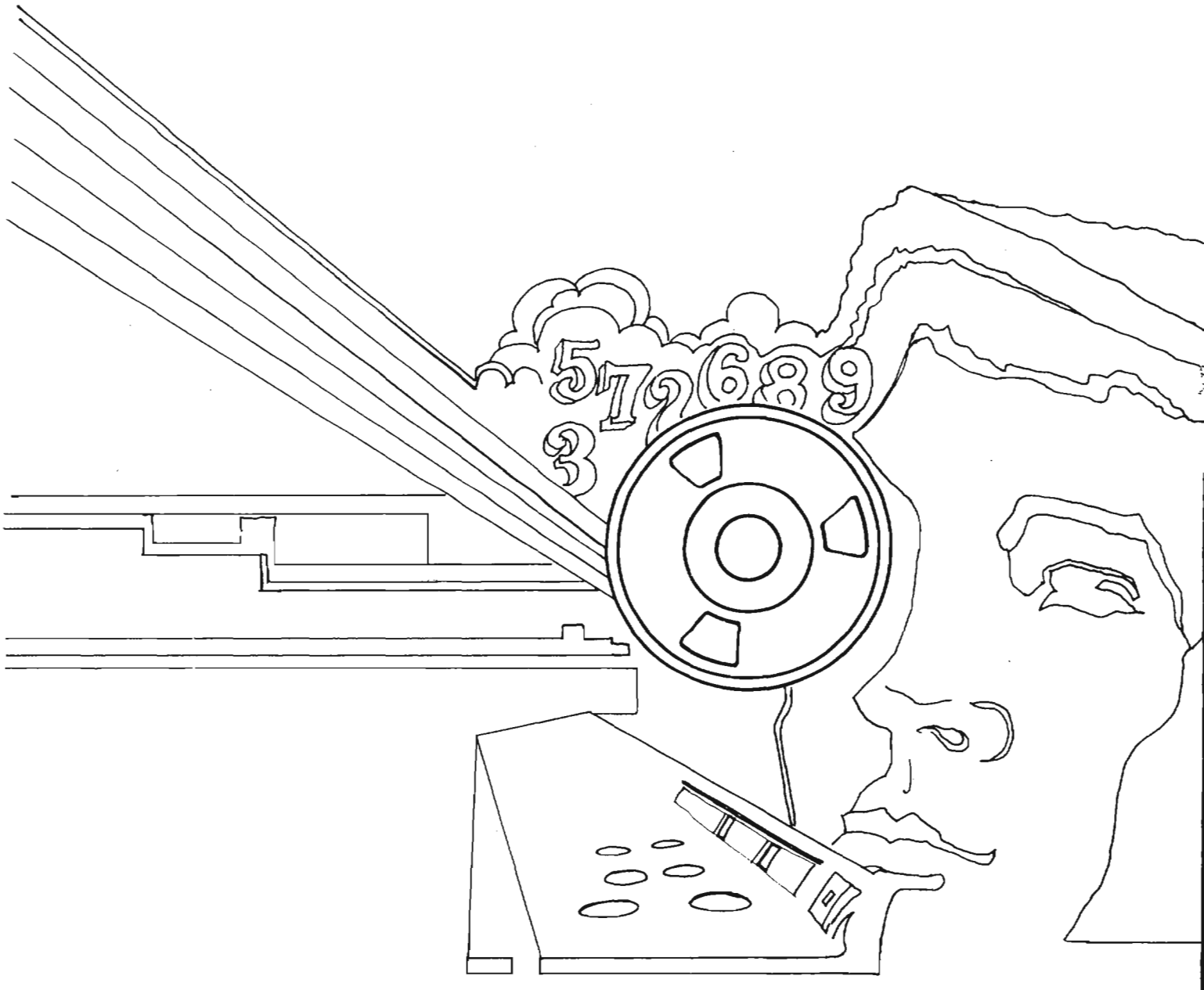
~~(FOUO)~~ To close, I would like to reemphasize that the operational side of ELINT is well appreciated in at least this corner of DDO (in fact, through out the organization, if the attendance of last year's Op ELINT seminar is any indication), that we recognize the fact that analysis of guidance triplets and jitter modes is best left to those who know them best (and possibly perpetuating [redacted] observation that ELINTers are misunderstood), and that in the analytic arena we should operate in concert, not opposition (although I am the first to admit that it very often doesn't seem that way).

[redacted]

P.L. 86-36



~~SECRET~~


5 7 9 6 8 9
3