DOCID: 4009937 P.L. 86-36

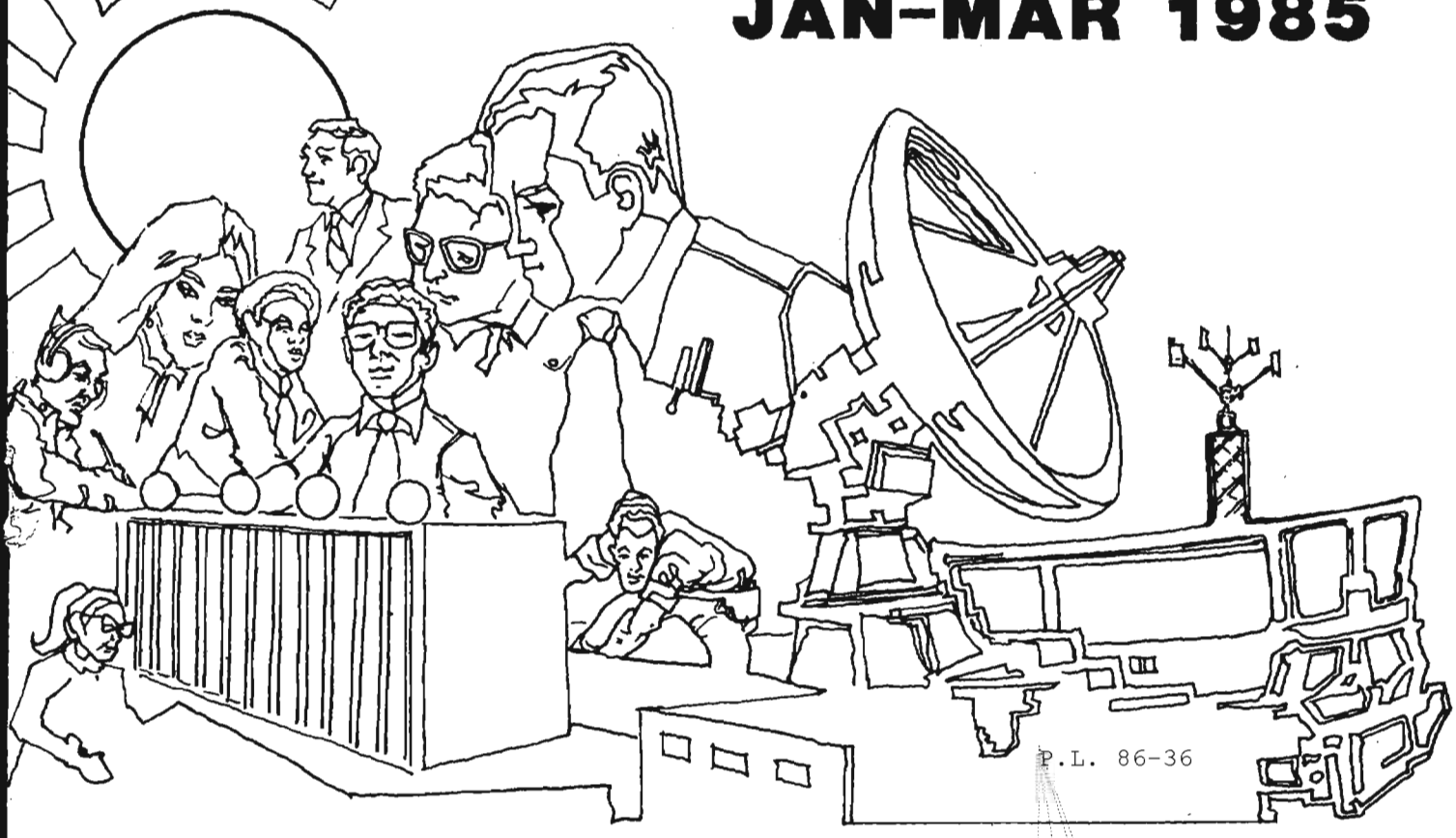
~~TOP SECRET~~

G51 [redacted]

TIONAL SECURITY AGENCY
T GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JAN-MAR 1985



P.L. 86-36

VIDEO TELECONFERENCING (U)..... [redacted] 1
LETTER TO THE EDITOR (U).....4
A MESSAGE TO CRYPTANALYSTS EVERYWHERE (U).....'THE MAD HATTER'.....5
I WOULDN'T HAVE MISSED IT FOR THE WORLD! (U)....Mary Ann Harrison.....6
SHELL GAME (U).....W.E.S.....8
BOOK REVIEW:
EASE MY SORROWS (U)..... [redacted] 9
BULLETIN BOARD (U).....13
A NOTE ON IMPROVING CRYPTOLOGIC RESEARCH (U)....Nathaniel C. Gerson.....14
FOOD FOR THOUGHT (U).....15
A TRAVELER'S TALE (U)..... [redacted] 16
TYME SHELL (U)..... [redacted] 17
ON EXCELLENCE (U).....18
FROM THE PAST (U).....19
NSA-CROSTIC NO. 60 (U).....D.H.W.....20

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

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

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

DOCID: 4009937

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XII, No. 1-3 JANUARY-MARCH 1985

PUBLISHER [redacted]

BOARD OF EDITORS

Editor..... [redacted] (963-1103s)
Production..... [redacted] (963-3369s)

Collection..... [redacted] (963-3961s)
Computer Security
..... [redacted] (968-8242s)
Computer Systems.... [redacted] (963-1103s)
Cryptanalysis..... [redacted] (963-4740s)
Cryptolinguistics... [redacted] (963-1911s)
Information Science
..... [redacted] (963-5711s)
Intelligence Research
..... [redacted] (963-3095s)
Language... [redacted] (963-5151s)
Linguistics. [redacted] (963-3896s)
Mathematics... [redacted] (963-5655s)
Puzzles.....David H. Williams (963-1103s)
Science and Technology
..... [redacted] (963-4423s)
Special Research.....Vera R. Filby (968-8014s)
Traffic Analysis..Robert J. Hanyok (963-3888s)

For subscriptions
send name and organization
to: [redacted] P14

P.L. 86-36

To submit articles or letters
by mail, send to: P1, Cryptolog

via PLATFORM mail, send to:
cryptolg at barlc05
(bar-one-c-zero-five)
(note: no '0' in 'log')

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

Editorial

[redacted] *retired on 31 December. During his stewardship as Editor he brought CRYPTOLOG into the contemporary world of word processors and electronic mail. He started with the UNIX system, then wrote innumerable shells specifically designed to do CRYPTOLOG layout. There are commands for the columnar format, for paragraphing with appropriate classification, for indented inserts, for "bullets," and for many other editing chores. There's a clever routine that allows the editor to make comments to the author via footnotes that do not disrupt the text. And there are even commands which automatically go in effect at specified off hours to execute the nroff-type shells for printing CRYPTOLOG.*

As a dyed-in-the-wool problem solver, Wayne also tackled the minor annoyances endemic to any computer system. He did this by writing many useful shells to smooth the way for the general UNIX user, and published them in CRYPTOLOG. An example of this type appears elsewhere in these pages.

Access to electronic mail has been a special boon to one set of people, that is, contributors in the field. By courier mail, whether air or surface, turn-around time for the usual sequence of submission, comment, review, etc., is too long to be practicable. Now, field contributors can get their articles to CRYPTOLOG via electronic mail faster than HQ people do using internal Agency mail!

Thanks, Wayne, and the very best to you from all of us.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4009937

VIDEO TELECONFERENCING:

can it increase

SIGINT productivity? (u)

P.L. 86-36

[redacted] **P11**

(U) Point-to-point video communication is clearly the next step on the road to teleportation ("Beam me down, Scotty"). Once face-to-face visual exchanges become routine, only the olfactory and tactile senses will remain to be remoted. Neither of these has wide usage in legally approved business transactions.

~~(C)~~ The increasing use of point-to-point video in the commercial world makes it important that the SIGINT community get some experience with this type of communications facility in order to make an informed assessment of its applicability to SIGINT operations. The question then becomes: can facilities of this type in fact increase productivity and the effectiveness of operations between NSA HQ and field units? To answer this question, P1 and T4 are jointly conducting a series of tests [redacted] the aim of which is to give a broad spectrum of working-level personnel, both at NSA and overseas, a chance to use video communications in actual operational exchanges.

~~(FOUO)~~ The following is a discussion of current technology and commercial applications of video telecommunications, and the results to date of the P1/T4 tests.

BACKGROUND

(U) Because of the pervasiveness of mass-media television, system designers and potential video telecommunications users in the business world have tended to focus on full-motion commercial television technology. But bandwidth requirements and dollar costs severely limit its use. Even with state-of-the-art image compression techniques, normal TV bandwidth of 45 megabits (Mbits) can be reduced to only 1.5 Mbits, or, reportedly, to 750 kilobits (kbits). Equipment costs per node with a fairly modest studio will run from $500k to $750k, that is, $1M-$1.5M for each two-station link. Space requirements, servicing, and management overhead add further direct and indirect costs. Annual communications costs for leasing fully dedicated channels bring total costs to an even larger figure.

(U) To avoid making this heavy capital investment, businesses are using AT&T video conference studio facilities. Cost for a half-hour video connection between New York and London is now $2000; between New York and Los Angeles $700. Only in a very small percentage of business transactions can such costs be justified. Further, even if the benefits of video conferencing are substantial, they are, for the most part, intangible. A using organization, therefore, must not only be large enough to pay the high costs, it must also be able to avoid close cost-benefit scrutiny. These facts effectively limit the user population for full-motion video facility to business officials at or near the chief executive officer level, to high-ranking government officials, and to defense-related applications of critical importance.

(U) Savings in travel costs are invariably cited by both video equipment manufacturers and by users of video conference facilities as the pay-off for video investment, but at a recent symposium on video teleconferencing it was generally agreed by participants who have actually used a video system that a great proportion of the trips "saved" would never have

P.L. 86-36

been made in the first place. It was also noted that many of the high-level executives for whom full-motion video telecommunications facilities had been acquired found them inconvenient and an unsatisfactory substitute for person-to-person contact. Phantom travel savings are nevertheless put forward regularly by operational users of video systems to demonstrate, in terms acceptable to in-house cost control authorities, that value is being received for money spent.

(U) Another type of video technology with much lower investment and operating costs is freeze-frame video. It is being used increasingly by business organizations to link working-level technical specialists at widely separated sites. IBM, for example, has a 60-site worldwide network set up primarily to serve programmer personnel.

(U) In a freeze-frame system, instead of sending 30 image-frames per second, as is the case in full-motion video, single images are sent at intervals which are a function of the bandwidth used. For example, when a 9.6-kbit voice-grade circuit is used, successive uncompressed color images (512 x 240 pixels, 6-bit resolution) can be sent every 78 seconds; with 64 kbits, a new image can be transmitted approximately every 10 seconds; and with 200 kbits, a new image can be sent every 4.5 seconds. With image compression software, these times can be shortened substantially, or, from another point of view, the bandwidth needed for a given refresh rate can be, at minimum, cut in half.

(U) Commercial applications have geared freeze-frame sales and applications to the telephone channel bandwidth, 9.6 kbits or analog equivalent. The resulting 78-second refresh rate is not suited to the easy interactive exchange of visual information, so use of the freeze-frame video image transmissions facility has been mainly as a graphics adjunct to an audio conference.

~~(FOUO)~~ Relatively unexplored up to this time, but now under study in the P1/T4 tests, is the question of whether a system with a video refresh rate in the 4- to 12-second range can be used to advantage in a general-purpose audio-visual communications link between working-level personnel.

THE TEST PROGRAM: [redacted]

(U) The impetus for undertaking the test program was the well-recognized phenomenon that temporary duty (TDY) assignments at overseas locations by working-level personnel are typically followed by an increase in the effectiveness of cooperation between the home and overseas elements and also by an increase in the information content of post-TDY messages and phone conversations. This appears to be the case even where, prior to the TDY, personnel in the respective organizations have spoken together regularly on the secure phone. It has also long been a fact of operational life that TDY budgets often fail to stretch much beyond the requirements of the "Chiefs" and very high priority projects, with little left for working level "Indians." Further, for a variety of reasons, it is often impractical to take productive personnel off ongoing tasks for a one- or two-week TDY trip.

(U) A second motivation for the tests was a two-sided one: a desire (1) to avoid getting caught up in the high-tech hype which usually accompanies the appearance of a new technique and too often generates imaginary and expensive requirements for "gold-plated" systems; and (2) to ensure that operational and intellectual inertia does not prevent timely acquisition by the SIGINT community of video communications if, in fact, such support would be operationally useful and cost-effective.

(U) The initial aim of the test, therefore, is to find out whether some of the benefits of TDY visits can be obtained by a video conference facility. Obviously, the closest analog to TDY would be a full-motion video facility; and just as obviously, the economic and communications costs point to freeze-frame technology.

TEST DESIGN

~~(C)~~ Test equipment, test configuration, and test sites were chosen with the following in mind:

- [] low cost
- [] adaptability to normal office environment
- [] manageability of equipment by users
- [] ability to test several refresh rates
- [] availability of communications bandwidth (on a temporary loan) between NSA and the site
- [] limited space requirements
- [] mobility of equipment
- [] reliability of equipment
- [] distance between paired locations. [redacted] agreed to be the first test site.

P.L. 86-36

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

DOCID: 4009937
E.O. 1.4. (b)
P.L. 86-36

(U) A simple (not compressed) freeze-frame video system in fairly wide use commercially was selected, with special options to allow operation at various refresh rates. Video bandwidth for the test was set at 192 kbits, and the audio bandwidths at 32 and 64 kbits. A special refresh-rate timing mechanism was incorporated in the equipment to allow examination of the usefulness/awkwardness of 40-second, 10-second, 6-second, and 4.5-second refresh rates. Test communications used bandwidths which had been installed and tested for operational projects but which had not yet come into full operational use.

~~(c)~~ The NSA mode shares a 11' x 20' area in P1 spaces, while the [redacted] mode occupied shared space in the mission conference room. The equipment, which is in wheeled cabinets, operates in a normal office environment, that is, without studio lighting or soundproofing, and needs no special technical services, so the conferees can manage the cameras and sound equipment themselves.

(U) The operational utility of the video system is likely to vary considerably from one application to another according to the type of conference, the numbers of people involved, and the conference skills and motivations of the participants. Each of following three types of video exchange requires separate consideration, so test participants are asked to conduct operational exchanges in each of them: 1) the stereotypic conference where two sides meet to iron out a problem; 2) a briefing or seminar format where one or more participants at one location make a presentation, with active questioning from the personnel at the other location; 3) a periodic assembly, similar to a staff meeting, of co-workers at the two locations to review matters of mutual interest.

PRELIMINARY FINDINGS

(U) a. In each of the above-mentioned types of video exchange, group-to-group communication is the key element; most one-on-one exchanges are adequately accommodated by secure telephone.

(U) b. In a normal office environment, discussing everyday work matters, and using video equipment of which they have hands-on control, conference participants to date have exhibited little of the stage-fright stiffness which vendors and commercial users of video systems have repeatedly mentioned as a major problem. It seems likely that the reported stiffness among commercial users is a side-effect of a studio atmosphere, which this test has carefully avoided, and/or of a slow refresh rate which might freeze for over a minute the picture of some person with tongue halfway out, or with eyeballs rolled; the faster refresh rate avoids extended displays of awkward postures.

(U) c. A pivotal question of interest in each type of conference has to do with a suitable image refresh rate. Looking to the possibility of standard operational deployment at major overseas sites, 32- or 64-kbit channels would be much more practical than 128- or 200-kbit channels. Preliminary results suggest that 4-second (192-kbit) and 6-second (128-kbit) refresh rates are not very different from a user's point of view; that a user can, with some difficulty, adapt to a 10-second (64-kbit) refresh rate, and that a 40-second (16-kbit) refresh rate is functionally more a facsimile system than a video system and is very awkward to use. A compression system, as noted above, could cut these rates in half.

(U) d. Audio quality sufficient to make the output of a speaker system easily intelligible to a group of conferees cannot be achieved at much less than 32 kbits.

(U) e. Allowing for a modest seating capacity, the minimum space requirement per node is 12' x 16'; group sessions of 8-12 people increase this requirement to 12' x 20'.

(U) f. The TDY savings to be realized from the use of video telecommunications are not likely to be large. The availability of a video link with a given station, can, however be viewed as a means of cushioning the adverse effects of a sharp cut in TDY funds for trips to that station.

(U) g. Loss of information attributable to the use of freeze-frame technology as opposed to full-motion technology has been minimal. When the refresh rate is either 4 or 6 seconds, there has been no apparent decrease of any significance in the usable (i.e. absorbable by the recipient) information-rate with respect to graphics. Also, with those refresh rates there has been no difficulty in establishing a well-defined personal "presence" for each participant in something very close to real time. Individual facial reactions and body language as well as local interactions between participants come across with only a mildly inconvenient delay. The nuances of facial expressions are of course lost.

(U) h. For the purposes of working-level exchanges, therefore, there appears to be little difference between the usable information carried by a full-motion video system and that carried by a quick-refresh freeze-frame system. If that perception is correct, there

are very few circumstances in which cost-benefit factors could justify paying the high costs of a full-motion video on long-distance links.

PROBLEMS IN MAKING ASSESSMENTS

(U) Reaching an objective conclusion about video cost-effectiveness is particularly difficult because the main advantages of video telecommunications are neither directly or discretely measurable. One typical test participant said, "This is great. I can't cite specific savings, but I can now show my workers who have never had a chance to visit this station exactly how the material they work with is acquired and processed in the field. They, and, in fact I myself, now have a much better idea of how this whole system operates." Based on that type of reaction, one observer might conclude that the video link is nice-to-have but not demonstrably cost-effective; another might claim that the pace of production and coordination tasks between the NSA and the field will increase enough to justify the costs of video communications.

(U) The basic problem is identifying what might or might not have happened if the video conference facility had not been used. It is likely that the best measure of cost-effectiveness will be an informed estimate by individual conferees of the length of time required to achieve an equivalent coordination of ideas between the conferring parties. User guesstimates, so far, have ranged from zero to two months. One to two weeks seems to be a figure of merit.

(U) Another problem which will make it hard for the community to reach an agreed-upon assessment of cost-effectiveness is the fact that a great many people (no correlation with grade-level discernible) have made up their minds either for or against the desirability or feasibility of video telecommunications before actually seeing it in operation. Some are convinced that video telecommunication is the overdue solution to a host of problems which have long plagued efforts to coordinate operations between NSA HQ and field units. Others are equally certain that video communications are a nice-to-have gimmick which can never justify the use of the communications bandwidth required ("Do you know how many 'grey lines' that is equal to?"). Still others take the position that as a means of sending graphics in support of an audio conference, a video system would be a great help, but that sending pictures of people would serve no real purpose. Since there is a full range of a priori opinions, someone must have it right, and, just as surely, the rest are in some degree wrong. The test series will, at minimum, narrow the area of disagreement.

PRESENT STATUS

~~(C)~~ At the time of this writing, tests with [redacted] are in progress. Present plans are to begin a 60-day test [redacted] in late February, and thereafter to shift the equipment to a site of a Service Cryptologic Element for the final test phase. A report summarizing test results will be published shortly thereafter. The report, together with the experience gained, should furnish a sound basis for decisions by the operating elements about whether to program or not to program for video telecommunications support.

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

Letter to the Editor

What a delight to read [redacted] *editorial!!!! To read that THE computer wizard was "thinking of ordering another file cabinet" gave me a good chuckle.*

Thanks, [redacted] *for making those of us who are definitely less-than-computer-wizards feel a little better about the abuse we receive from those inanimate objects, be they hardware, software, connectors, or whatever.*

Mr. Sawyer's and [redacted] *articles were also excellent and too true.*

Thanks for a fine issue of CRYPTOLOG.

[redacted] *B12*

P.L. 86-36

	A	M	E	S	S		A	G	E	T	O			
	C	R	Y	P	T		A	N	A	L	Y			
	3	T	S	E	V		E	R	Y	ω	H			
	E	R	E	F	R		O	M	T	H	E			
	M	A	J	H	A		T	T	E	R	X			
											(U)			

~~(FOUO)~~ MADCAPS is here at last! It's a continuing project to assist cryptanalysts working on manual systems. The purpose is to collect, document, organize, and invent diagnostic programs, and to make them available on supercomputers and on Agency Standard Terminal Workstations. The project, though informal, is blessed by upper management, and is staffed by a steering committee, a working group, and cryptanalysts at large:

[] steering committee = TOPCAPS = will provide continuity;

[] members of the working group = MADCAPS = will be assigned for short tours from various offices throughout DDO.

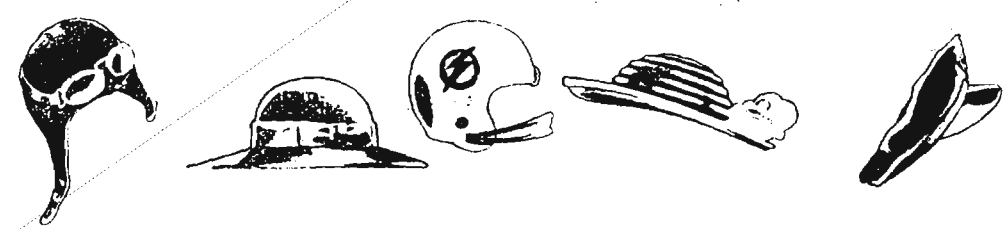
[] cryptanalysts at large = THINKING CAPS = That's you!

(U) Among the services that MADCAPS will be providing are: supporting the DPP in the TCAP main tube room; assisting users personally; developing a training course in conjunction with the NCS; and holding tea parties (seminars) for programmers.

(U) So, THINKING CAPS, let the MAD HATTER hear from you after you have tried these programs. As the MAD HATTER refuses to be identified, send your comments to the CRYPTOLOG editor; she has agreed to give space for this exchange and to act as intermediary pro tem.

(U) Is there a cryptanalyst around who likes to write and is willing to take on the CRYPTOLOG exchange?

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



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

I Wouldn't Have Missed It for the World!

(u)

Thoughts on the Senior Executive Fellows Program, John F. Kennedy School of Government, Harvard University, September-December 1984

Mary Ann Harrison, A67

(U) The Senior Executive Fellows (SEF) Program is designed to provide training for high-level managers in public sector organizations, to assist them in improving their management skills and techniques, and to add to their understanding of the issues and institutions which shape the governmental working environment. The program's major goals, to quote from a Kennedy School brochure, are:

* To challenge participants to step out of their prior professional identities and to think concretely and analytically about themselves as executives;

* To expose them to historical, institutional, and thematic perspectives that will deepen their knowledge and understanding of the public manager's larger operating environment;

* To train them in essential cognitive and behavioral skills that will enable them to operate more efficiently and effectively;

* To encourage them to reexamine old assumptions and to assess their attitudes, values, and beliefs in light of new and increased public responsibilities;

* To inspire them with a sense of pride and confidence in the practice of their profession, through an awareness that public management demands the best efforts of talented people, that it is socially important and personally rewarding.

(U) The thirteen weeks I spent in the program this past fall convinced me that, in all respects, the Kennedy School has overfulfilled its plan.

(U) Our SEF class comprised forty students; we represented two state governments and more than 25 federal departments. The Kennedy School provided apartments for us (save for two Army men who were there as part of another program and were required to find accommodations on their own) and meals were furnished on most days. Many of the books used in class are ours to keep; other books could be purchased, usually at discount, at one of the many excellent bookstores in the Cambridge area. (It is said that, outside of buildings belonging to Harvard, all buildings in Cambridge are either clothing stores, book stores, or restaurants; some seem to be all three at once!)

(U) Our class spent two hour-and-a-half sessions with an internationally known authority on the art of negotiation, a man who helped hammer out the Camp David accord between Begin and Sadat. We had ten hour-and-a-half sessions on leadership with a man who is a psychiatrist, musician, philosopher, and a highly creative teacher. We examined the attack on the Marine barracks in Lebanon with the only civilian to serve on the Long Commission, which investigated that tragedy. We also studied:

* micro- and macro-economics;

* the uses and misuses of statistics;

* the whys and wherefores of computers and management information systems;

* how to deal with the press;

* how to deal with lawyers;

* what makes McDonald's more successful than

Burger King;

* the Richard Helms perjury trial;

* how to organize a public service organization so that it truly does serve the public;

* the features of the "Japanese management style" that perhaps could/should be adopted by U.S. business;

* the relationship between the Executive and Legislative branches;

* the growth of Presidential staffs and their influence;

* the effect on world politics and economics of multinational corporations;

* crisis management, using the Cuban Missile Crisis as an example;

* competition and regulation in U.S. business;

* decision analysis: what it is and how to do it.

We also discussed our own strengths and weaknesses as managers and what it means to manage in the public sector. This list includes only the highlights of our studies; I hope it gives some idea of the diversity of the program.

(U) The predominant method of instruction was the case method, "a teaching technique which requires a high level of involvement by participants." The brochure goes on to say:

> The success of case teaching depends upon the full participation of each class member and demands thoughtful analysis and active contribution to class discussion...the entire class explores the case under the guidance of the instructor. Typically there is no "right" answer; participants must be ready to defend their analyses and conclusions against the total experience of the class. The instructor serves as catalyst, devil's advocate, and moderator in leading the class through the analysis to a workable solution. Analysis of real problems and learning by vicarious experience are the essence of the case method. It puts the burden of learning on the participant, who gains a new level of understanding of the complexity of public decisions.

(U) Although the size of the class precluded as much dialogue as many of us would have liked, the intellectual exchanges were usually lively and interesting.

(U) For the first hour of each day we met in groups of eight, to discuss the day's cases and to experiment with the dynamics of small-group decision making. Each of us gave his or her own case study during the semester, typically a description of a management problem each of us was facing in our own jobs, with the hope of eliciting suggestions and solutions from our seven "groupmates."

(U) Shortly before Thanksgiving the SEFers were assigned in pairs to work with small groups of first-year graduate students in an exercise on cutting the food stamp program. The groups were responsible for creating a briefing book proposing alternative ways to reduce the food stamps budget, with recommendations for action. They then briefed a present or former Health and Human Services official involved with food stamps. This exercise was, for me, one of the highlights of the semester.

(U) After the conclusion of the food stamps project, several graduate students asked some of the SEFers to participate with them in a seminar on the ethics of the workplace. "To Resign or Work Within" was the topic, what to do when you are instructed to do something that runs counter to your personal sense of right and wrong. The discussion was interesting and exciting; I hope the graduate students got as much out of it as the SEFers did.

(U) The official SEF program ran from 8:00 to 12:00, five days a week and most Saturdays. Afternoons were open for the SEFers to audit any course they chose, graduate or undergraduate, at Harvard (Kennedy School, Business School, Law School, etc., anywhere the professor allowed auditors), Radcliffe, Massachusetts Institute of Technology. I audited two courses: Communications and Information in Foreign Policy; and Current Issues in American Foreign Policy: Managing the Superpower Relationship. Some of my classmates audited courses in psychology, Japanese history, poetry, computer science, even one very unusual class entitled The Beast in Literature!

(U) Fellows of the Institute of Politics held weekly seminars on such disparate subjects as the future of liberalism, the Arab-Israeli conflict, the contemporary right, social welfare policy in the 80's, and criminal justice. They were informal meetings; one could simply drop in on whatever session sounded interesting that particular week. The caliber of guest speakers is indicated by the fact that the liberalism seminar heard from the former Prime Minister of Canada, Pierre Elliott Trudeau, and from David Steel, Leader of the British Liberal Party.

(U) The SEFers also had occasional dinner guests, people who were scheduled by the SEF program coordinators, or who were suggested by us, the students, as interesting folks who had something to share with our classmates. Included in this group were an expert on the Far East who had some fascinating information about the origin and development of the Chinese civil service; a witty refugee from the Harvard Business School who talked about management information systems; and one of the leaders of the foreign policy seminar who gave his thoughts on what's ahead for the second Reagan administration.

(U) Speakers at the Kennedy School Forum included Zbigniew Brzezinski, Daniel Yankelovich oi Yankelovich, Skelly and Wright, and J. Peter Grace of the Grace Commission. These seminars were open to all, and if you didn't claim a seat by 7 o'clock (for an 8 o'clock speaker) there was standing room only!

(U) As members of the SEF program, we received Harvard Student Cards which entitled us to use all Harvard facilities - libraries, gymnasiums, swimming pool, theaters, museums, etc. Some of my classmates learned how to row (crew? scull?) and renewed their swimming skills as they retrieved themselves from the Charles River after their boats capsized!

(U) Much of what I learned in the SEF program can be applied at once: how to be a better manager, how to be a better subordinate. Some of my newly acquired knowledge probably won't come into service until later: how to design organizational strategy, how to marshall resources and support. But all of the SEF experience is an important and valuable part of my professional "tools of the trade."

(U) I envy the next NSAer who becomes an SEFer. I'd like to do it all over again!

SOLUTION TO NSA-CROSTIC No. 58

[redacted] "The Islamic Time Bomb," CRYPTOLOG, December 1983

"What are the objectives of the new Islamic revolution?

"The elimination of undesirable or immoral behavior such as gambling, [drunkenness,] prostitution, pornography, and corruption;

"The conformity of secular law with Islamic law; and

"The establishment of Islamic governments."

Shell Game (w)

WES

(U) The other day, I got a note from a reader over the network titled "Asleep At The Switch," apologizing for not having answered a message I had sent him. I had sent the message to his personal account, but he was in the habit of logging in to the group account on his host computer and so hadn't seen my message for several days. That's a common problem when people have group accounts as well as personal accounts.

(U) This magazine is done on a group account, and it is easy to forget to check for mail in one's other account. For that reason, we have set up the file that runs automatically whenever you log in called ".profile" so that it checks for mail in the companion accounts. For example, the ".profile" for CRYPTOLOG's group account looks something like this:

```
if -s /u6/wes/.mail then
        = b 'There is '
else
        = b 'No '
endif
if -s /u2/hes/.mail then
        = c 'There is '
else
        = c 'No '
endif
pump
        $b mail for wes
        $c mail for hes
!
```

(U) Over on my personal account, the .profile contains similar instructions to check the mail file in CRYPTOLOG's group account.

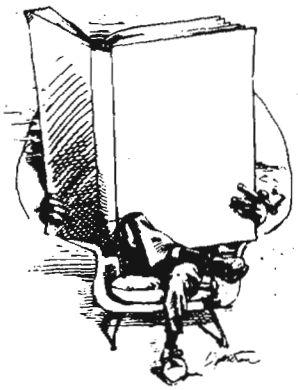
(U) We have learned to put this command at the end of the .profile, so that it is one of the last things to come up onto the screen after logging in. That way, a long "message of the day" doesn't push this mail notice off the screen.

(U) By the way, if you ever need another look at that "message of the day" it is always available with:

cat /etc/motd

P.L. 86-36

DOCID: 4009937



BOOK REVIEW

(u)

P.L. 86-36

[redacted] **P13**

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

Review:
Ease My Sorrows
by Lev Kopelev
Random House, NY, 1983

~~(TSC)~~ In early 1950 Alexander Solzhenitsyn was abruptly transferred out of a job of evaluating the intelligibility and security of Soviet analog telephone scramblers, to a dull mathematical job in cryptographic design, because he had proved that a voice scrambler designed by the KGB head of the research lab was the worst of the candidate cipher machines. After that the evaluation work fell apart, with profound results for the USSR [redacted]

(U) Lev Kopelev was the linguist in a small three man team, including Solzhenitsyn and the engineer Dmitri Panin, who had pioneered in Soviet work in speech analysis, building their own sonogram, and developing new equipment, concepts and techniques for the analysis of Russian speech. With the other two, he was imprisoned in a "sharashka," a high class prison for technical workers, in the Marfino suburbs of Moscow.

(U) In his book The First Circle, Solzhenitsyn first described the Soviet speech research and cryptography at "Mavrino." Kopelev was the character Rubin in that book. This new account illuminates many new aspects of the Marfino work and the prison life. Ironically, Solzhenitsyn has revised part of The First Circle (the voice recognition spy hunt) to conform more closely to Kopelev's account.

(U) The Marfino sharashka was housed in a former church with the name Ease My Sorrows, and run by the KGB (called MGB in 1950). All three men, and most of the other prisoners, had been convicted of violations of Article 58 which covered terrorism, espionage, sabotage, and other acts against the State [p.46]. Solzhenitsyn had been captured by the Germans. Kopelev had tried to restrain rape and pillage by troops under his command in Germany in 1945. Panin was arrested in 1940 for "conversations," and then sentenced while in a Russian prison in 1943 for "defeatist agitation." In these trials the accused was usually not present and had no right to defend himself. Kopelev, a Jew, had served with front line troops, and was an ardent Stalinist, even in prison.

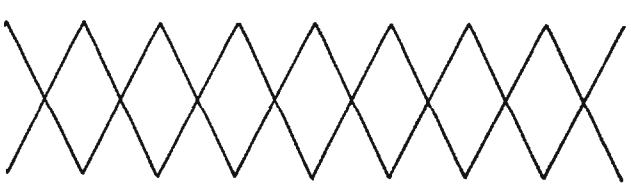
(U) There were numerous sharashkas, and they represented an idea that only Stalin could have thought up, where the political prisoners with special skills such as engineers, mathematicians, etc. could serve the state by conducting useful research. Airplanes, radars, and many other high technology products were designed and developed in the various sharashkas, where the conditions, though severe, were far better than the forced labor camps in Siberia, or the uranium mines. The prisoners, called "zeks" in prison slang (from a contraction z/k of zakliuchennyi), knew when they were well off, and worked with the greatest intensity to avoid being sent to a labor camp, where they would die. In the prison environment there was not much to take their minds off work and so Stalin got a maximum effort from these scarce scientific

resources. Tupolev, the aircraft designer, was arrested in 1938, worked in a sharashka, and was released in 1943.

(U) The sharashka at Marfino was engaged in speech engineering and encryption. In addition to the Russian zeks, there were German POW's, many of whom were very gifted and industrious, KGB administrators, such as Anton Mikhailovitch V. [Vasleyef], a KGB colonel, some Russian "free" workers, and various Germans, Czechs and Austrians who had been arrested and charged with espionage because the Soviet research programs apparently needed their skills.

(c) Technology transfer was an important foundation for the lab's activity. The Philips lab in Berlin was dismantled and moved to Marfino. The technical library, a key element, was made up of Soviet technical books and of war spoils: German, British, French and American scientific journals [p.16]. This was augumented with linguistic books, and books of literature and poetry, which Kopelev said he needed for linguistic research, but actually valued for their culture and intellectual inspiration. An uncommon prison library.

(c) Colonel Mikhailovitch supplied them with stacks of British and American journals on acoustics. Fletcher's Speech and Hearing was the foundation of their work. The published American work in spectrum analyzers was adapted by Kopelev, Panin, and Solzhenitsyn to create a visible speech recorder of their own [pp.50-51]. This single instrument played a crucial role in both speech recognition and cryptographic evaluation, but its potential was inevitably thwarted by the realities of prison existence.



(U) The basic idea of the speech scrambler was based on German and Allied wartime speech coding which split the voice channel into several subbands by filters, wrote these sub bands on a magnetic recording disc, and then picked them up in short segments of 150 milliseconds, with mixing of the time-frequency segments by a "coder." This signal was sent down a telephone line, and then decoded and reassembled at the receiving point. The KGB lab chief Anton Mikhailovitch V. (the prototype of Yakonov in The First Circle) originally spoke of absolute security for this system, in 1948 [p.35]. The zeks were promised rewards and early release if they succeeded, and some actually did get reprieves and big cash awards [p.140].

(c) To provide a foundation for the work, Kopelev, Solzhenitsyn and Panin undertook new linguistic research, identifying Russian spoken syllables and their frequencies. From these data, they developed various methods of evaluating how well scramblers preserved the information bearing elements of speech. This linguistic work was a novelty compared with the "engineering" method of treating speech merely as a waveform. Kopelev tried to get his discoveries published in someone else's thesis, but various reorganizations of the sharashka led to the destruction of all his data, the breakup of the team, the discrediting of sonograph analysis, and a general frustration of all this important cryptologic work.

~~(c)~~ The top secret sonograph (phonoscopy) work was disbanded, and Kopelev and a few others were put under a major Federovitch K., who was a serious mathematician and engineer. The speech coders could be solved by intensive human effort, ranging from 120 to 600 minutes per minute of speech. Kopelev used sonograph pictures to decode the mosaic coded speech, and came to the conclusion that they could be quickly read by the Americans, with their better equipment [p.137]. A fellow zek warned them they were sawing off the branch they were sitting on, and would be sent to the mines if they showed that the sharashkas's work was worthless. KGB Major Federovitch decided that the mosaic coders were needed by the state, they were better than nothing, and prevented simple wiretapping, and the sonograph decoding could be done "only under laboratory conditions." He then sent Kopelev back to the acoustic lab, away from scrambler evaluation [p.138].

~~(c)~~ In addition to the analog "mosaic" coders, Kopelev also mentions a "superdependable 'impulse' coding" [p.155]. Since "coder"

DOCID: 4009937

means enciphering device, this implies that digitized speech encipherment was also being worked on at Marfino, but he does not elaborate. The impulse coding thwarted his attempts to recreate the characteristics of a voice.

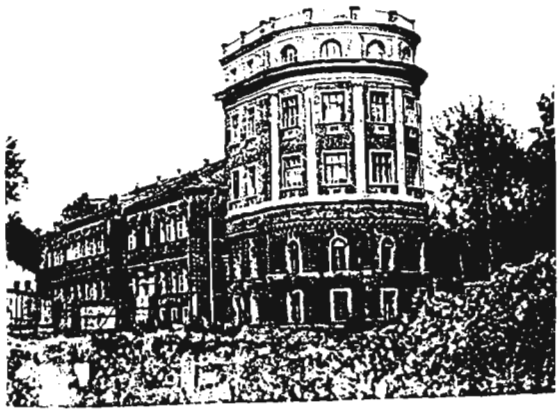
(U) Kopelev noted, in leaving the mathematics group, that all the desks were open--all surfaces in view--and every task precisely defined; you couldn't get sidetracked [p.138]. This strict environment apparently suited the KGB managers, who had arrived at their positions in charge of the cryptologic work by torture and assassination, but the zeks (who were the Soviet cryptologic technical track) were intellectuals and scientists who not only found this stultifying, but frustrating to their abilities and to the mission of the sharashka [pp.154,161].

(U) The sonogram that Panin, Kopelev and Solzhenitsyn developed was also applied to a spy hunt, in one of the illuminating episodes in the book. In the fall of 1949 a wiretap on the US embassy recorded a Soviet speaker trying to tell the Americans that a US scientist would shortly pass atomic secrets to a Soviet agent in New York [p.73]. The problem was to identify who made the telephone call. Several suspects had their conversations recorded, and Kopelev, who was best at reading the sound pictures, tried to identify the right suspect.

(U) A new secret sonogram laboratory was instantly established in the sharashka. The zeks had to take a secrecy oath, which authorized them to be shot without a trial [p.76]. Kopelev told Solzhenitsyn about the project, but Solzhenitsyn warned him not to tell anyone else. The zeks described the taped informer as a "bastard." Solzhenitsyn shared Kopelev's disgust with the man who called the Americans, and called him "bitch," "viper," "whore" and so on. When questioned, the informer, a Soviet foreign service official, denied calling the Embassy, but Kopelev and the other zeks had the satisfaction of helping the state convict him. They denounced him for giving away information about the atomic spy contact. The suspect had had all the advantages of Soviet life, and had been in Komsomol as well, with family Party connection. They despised him.

(U) It is hard to imagine Americans imprisoned for political crimes, (such as being POW'S) being such patriots in reinforcing the power of the police. [1]

(U) This counter-espionage success made the sonograph work important to the KGB, and the



The sharashka in Martino on the outskirts of Moscow, formerly the church, "Ease My Sorrows"

zeks were praised. Soon after new tapes arrived. Some Soviet Army tank repairmen had called the US embassy as a prank, pretending to have information to pass. A sergeant's notebook was found with some data about tanks and their state of repair and other military facts. The sergeant confessed, and said he was just trying to bluff the Americans. However, Kopelev discerned that three buddies were in the scheme, and that the man who confessed was not the one who had called the embassy. Realizing that the accused sergeant had behaved selflessly, taking all the blame to protect his buddies, Kopelev fudged his results. He could have exposed the truth, and gotten long sentences for three soldiers rather than one, and this would have confirmed the value of sonogram speaker identification, but he knew that evidence of a "collective" crime would be much harder on the men. The KGB supervisor Mikhailovitch was furious, because he had ballyhooed the sonograph discoveries, and then had no new success. This discredited the sonograph.

(U) In this second incident, Kopelev sympathized with the "spies," and protected them as well as he could, at the cost of discrediting his work, because he didn't think they were truly enemies of the Soviet state.

(U) When the sharashka was taken over by a new KGB officer in 1950, it was also transferred administratively from the MGB to the Directorate of the Central Committee of the Party [p.154]. To tidy up for the transfer, anything not included in the inventory that covered the transfer was ordered destroyed. This was a catastrophe for the project. Hundreds of thousands of irreplaceable foreign documents, and priceless equipment including a 70,000 Mark Zeiss microscope, were burned and smashed and thrown in a pit by the enthusiastic KGB staff. All Kopelev's sonographic data and research materials went. Zeks could no longer be authors or sign anything. Controls were tightened. [pp.151-4]

(U) In spite of his prison sentence and treatment, Kopelev remained a dedicated Stalinist, rationalizing even his own fate as historically inevitable. "We are on a train, bound for socialism, and only the stupid guards have put us in the prison car." His fellow zeks replied, "We are going nowhere, mired in shit, and you call it honey".

(U) Kopelev tried to defend Stalin's brutal policies and actions even after his death, but got heated arguments from other prisoners [p.224]. Gradually he concluded that the punitive actions of the NKVD, MGB, and OSO in the prison camps were senseless and useless, rather than part of a historical pattern. He began to think about God. He came to realize that Stalin had not been a major historical figure, because the system rejected his methods and henchmen and discredited his memory, almost before the corpse was cold.

(U) One of the most interesting points about the book is made in the foreword by Robert Kaiser, former Washington Post correspondent in Moscow, who knew Kopelev during his assignment. The Russian intellectuals began with the assumption that a reporter from as important an newspaper as the Post would not only speak Russian fluently (Kaiser's Russian was not bad), but would be familiar with all of Russian literature, and would know who all the key people in Russian intellectual life and publishing were. They were disappointed in this assumption, but still clung to the belief that at the least, the reporters and their wives would be completely familiar with all the important works in German literature, or at the very least, American literature. Alas! The Russian intellectuals knew not only all their own literature, but were taken aback when the Kaisers could not answer their searching questions about the meaning of this and that element of American literature. Kaiser remarked that Russian intellectuals "are serious about their work." [p.viii].

~~(C)~~ Therein may lay the key to Marfino and its gifted zeks. Kopelev, Solzhenitsyn, and many others were intensely educated people, who carried their passion for knowledge and intellectual endeavor into every situation. Kopelev, the loyal Stalinist, tried to rationalize the whole prison system and his own treatment as historically inevitable. Solzhenitsyn attacked the gulag system, and the whole Soviet state, as an outrage against democracy and the Russian people. Inside Marfino, they and the other zeks worked intensely to serve the state, as loyal Russians. They struggled to create a work environment in which they could carry on discussions of literature, art and politics, while they worked--and resisted the efforts of the sharashka managers to narrow them to routine prescribed tasks. Being an intellectual was a full time task, even in a prison.

~~(TS)~~ [redacted] the MVD managers of Marfino were as stupid and shortsighted as they were, so that they largely wasted the scientific and intellectual talents of the people they arrested and put to work on speech encryption. The zeks knew their efforts were being frustrated, but in the end were unable to keep the important research going, or stop the production of deficient cipher machines. This waste of ability by a despotic government seems to have persisted for a long time in Russia, with anguish and hardship for the people who understood the situation best. No wonder that a church was named "Ease My Sorrows."

SOLUTION TO NSA-Crostic No. 59

"Naming Soviet Cities," VOX TOPICS, Vol 11, Spring 1984

"A noticeable trend in Soviet city naming began with the death of Lenin: important cities were renamed for deceased Bolshevik heroes. It was [extremely] fitting that after Lenin's death, his birthplace and the place where the revolution erupted should be named for him.

DOCID: 4009937

BULLETIN BOARD (u)

FIELD STATION MAIL

* Sending mail to co-workers who are now in the field is not hard when you know when and how. What you must not do is forward mail, because some items cannot be sent to certain field sites. The thing to do is to return the mail to the sender, with a note to the effect that J. Schmoe is now at Fxxx. Then it's up to the sender to check it out. If you're the sender, and it's permitted, consult these NSA Regs: R10-04, Armed Forces Courier Service; R10-12, Personal and Personally Addressed Mail; R10-27, Official Mail. Your Staff Security Officer can help you interpret these Regs. What not to do? Pop it in a shotgun envelope. Never, Never, Never!

SPEAKERS OF FOREIGN LANGUAGES

* Can you speak a foreign language with native or near-native fluency? If so, please make yourself known. On a piece of paper write your name, language(s), organization and secure phone number, and send it to [redacted] P16.

P.L. 86-36

FILBERT FOR CRYPTANALYSIS

* Attention, hand systems cryptanalysts! Do you have an IBM PC, XT, or ASTW? Are you tired of having to go to the tube room to do a short run? Consider FILBERT. It's a set of routines for the pc designed to help with the diagnosis, recovery, and exploitation of low-level manual systems, and is intended as an adjunct to the mainframe rather than a replacement for it. The CA techniques implemented on FILBERT are the established, tried-and-true routines familiar to cryppies. FILBERT is available through the PCIC (Personal Computing and Information Center) in the main library, or call P13 (963-5868) for more information and/or a demonstration.

FILBERT USERS

* Notice to current FILBERT users: FILBERT version 2.0 is now available. It incorporates changes, upgrades, and additional programs, all as a result of your input. Thanks! If you have not been contacted about receiving the new version, call P13 on 963-5868.

CODE WANTED

* Wanted: a small operational code of 1000 groups or under to be used for training purposes, as is or disguised. The code may be one-part or two-part, preferably, in a language other than English, and need not be well recovered. It should be unenciphered, or if enciphered, the keys provided as well. Either hard copy or machine-readable traffic can be used, 25 messages or more. A bennie is that bookbreaking programs for that code will be developed for a PC. For further particulars call [redacted] E42, 968-8418.

P.L. 86-36

LINGUIST PC USERS

* Special for linguists who use computers: As personal computers and workstations become more widespread throughout the Agency, some of you are modifying or developing your own programs to aid you in your daily work. In order to establish a clearinghouse for existing software and to share ideas for software tools, P16 is establishing a users' group for linguists and reporters interested in software packages for foreign languages. A description and demonstration of [redacted] a multilingual terminology retrieval and maintenance system available for the IBM PC will be presented at the first meeting, scheduled for the last week of May, specific time and location to be announced. All Green and Orange badgers are invited. Point of contact is [redacted] P16, 963-1103.

TELECOMMUNICATIONS TERMINOLOGY

* Just out! Hot off the press is the Glossary of Telecommunications Terminology. It was prepared by the Policy and Liaison Staff of the Telecommunications and Computer Service Organization, with the assistance of the National Data Standards Center, and carries an overall classification of CONFIDENTIAL. For copies call or write [redacted] P13D, FANX III, 968-8162s.

P.L. 86-36

A NOTE ON IMPROVING CRYPTOLOGIC RESEARCH (u)

Nathaniel C. Gerson,

W36

(U) Following is a suggestion for improving cryptologic research in the fields of physics, engineering, and computer technology. It involves:

(a) defining a strong relevant program, and
(b) insuring that it will be carried out.

DEFINING RESEARCH GOALS

~~(FOUO)~~ The first step requires the formulation of an overall, cryptologically-related research plan. Such a plan may evolve either by inclusion in "SIGINT 2000--TECH FOCUS" or as the result of an internal seminar specifically held for this purpose. In the latter case, the seminar could be of five days' duration to an audience consisting of middle managers responsible to DDR, DDC and DDO. Presentations would be made as follows: during the first two days, operationalists would outline their immediate and projected technical problems and indicate the relative importance of each problem. On the second two days, researchers would describe their current ongoing investigations and provide their views on how these studies impact on operational problems. On the final day the audience would attempt to draft mutually agreeable research objectives. If the final day produced even a single draft plan, the seminar would all be worthwhile. In any case, it would be illuminating to the management.

(U) An intangible objective of the seminar would be to initiate a frank dialogue, long overdue, between the Operational and the Research elements of NSA. (I sometimes wonder whether contractors attending the annual Defense Intelligence Technical Forum do not, in fact, gain a better understanding and appreciation of cryptologically oriented research than do personnel in R!)

(U) In any event, if an internal seminar on research were held, it would be desirable to allow ideas to gestate for four to six months. Thereupon a very small number of knowledgeable individuals of those attending the seminar would be tasked with defining a cryptologic research program. About every three years thereafter critical reviews of the total program would be necessary to examine pertinence, quality, and progress. It is imperative to note that applied researchers have a dual obligation: to originate investigations directed to the parent agency, and to put an end to unpromising lines after an honest trial period. It should be understood that only short- or intermediate-term research would be undertaken; long term investigations (of second, third, etc., order effects) are properly the province of other institutions, such as the National Science Foundation.

ORGANIZATIONAL RESTRUCTURING OF RESEARCH

~~(C)~~ A serious question should be raised as to whether the present arrangement of placing research in R is conducive to progress. In R, research is somewhat concentrated in R1, mainly for COMSEC, and R5, mainly for COMINT. (Minor research projects are underway in other elements of R as well as in S, T, W, etc. These efforts need not be considered here.)

~~(FOUO)~~ The primary thrust of R as it exists today is that of a technical contracts group. It easily could be called TECON or some other name and its function would be unchanged. To place matters in perspective, we might note that the current activities of R comprise about 90% technical contracting and 10% research.

~~(FOUO)~~ The principal difficulty facing NSA is the relationship between the problems identified in Operations and the manner in which they are investigated in Research. Moreover, referral of problems from Operations to Research is hindered by organizational barriers, among other things. Also, the formal flow of updated information from DDC and DDO to DDR is apt to be slow and ponderous. These factors mean that the relevance of on-going research in NSA gradually fades as R continues to work on problems which are of interest only to itself. Thus money is spent to no advantage, but spending gives an illusion of progress.

~~(FOUO)~~ Restructuring the research effort organizationally might be a method of removing some of the present built-in obstacles. One way would be to put R1 to under the jurisdiction of DDC and R5 under DDO, both as staff elements reporting directly to the appropriate deputy director. Another might be to combine R1 and R5 and form a new element at the directorate level.

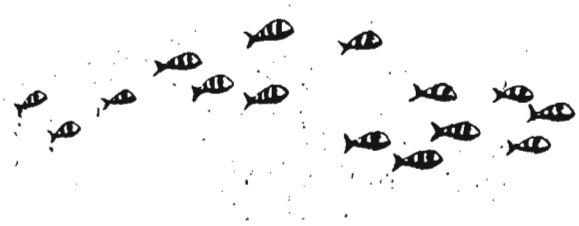
(U) Either of these arrangements would permit the detachment from day-to-day operations that is necessary for research, yet allow the control needed to insure that the research is relevant and cryptologically oriented. Also, it could better shield the research from some of the wild disruptive fluctuations in funding. Research would become more meaningful, and NSA would be less likely to be taken by technical surprise.

EDITOR'S NOTE

~~(FOUO)~~ As we go to press, we learn that R1 has just been transferred to DDC.

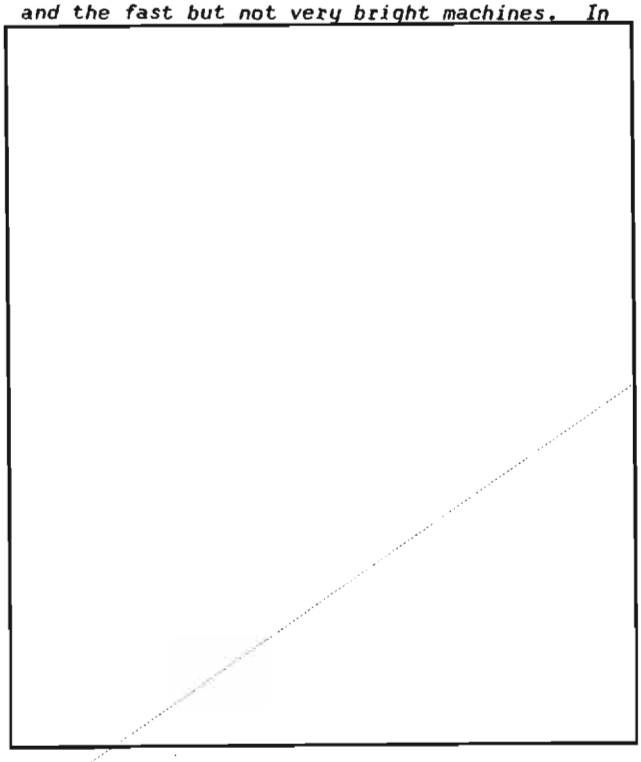
FOOD FOR THOUGHT

(u)



Extract from "General Utility Programs for Cryptanalysis" by Carolyn Palmer, published in Collected Papers on Cryptanalytic Diagnosis, NSA, April 1969 (S-194,074)

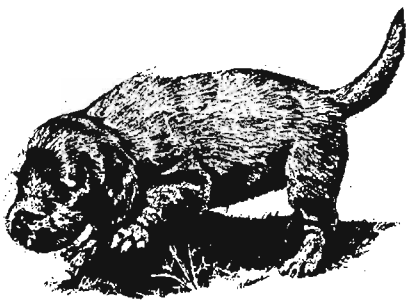
~~(S-CCO)~~ There is another factor which, in my experience, has always been necessary for reaching a successful conclusion to any problem complex enough to require a series of machine processing steps. This is continuous interaction between intelligent human beings and the fast but not very bright machines. In

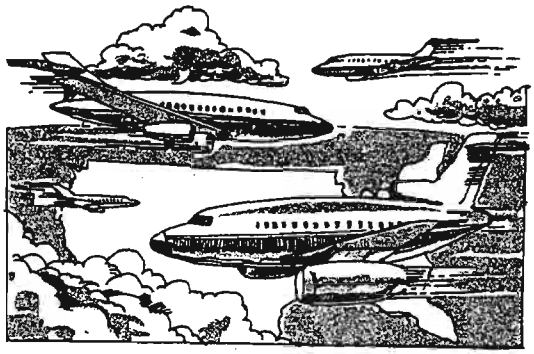


EO 1.4.(c)
P.L. 86-36

OCID: 4009937

A Traveler's Tale (u)





P.L. 86-36

The trip was planned as a nice spring TDY to Oak Ridge, Tennessee. Of course, spring in Oak Ridge is not necessarily spring in Baltimore, and I watched in horror as the fog rolled in the day I was to leave. The ticket agent at BWI postulated that if any airport open for outgoing flights, it would be National. O.K. Take a limo to National, have a nice lunch except for a funny twinge of pain whenever chewing anything hard. Oh well!

Wait several hours at National. Finally the announcement comes that the plane is on the ground at Dulles. They load us on a bus and take us to Dulles. We're only running 6 hours behind!

We take off at last, but not before the stewardess intently examines the "What To Do In An Emergency" card. (Is this her first flight??) The pilot announces "Please keep your seat belts on, we're headed for a little turbulence." KA-BOOM! The cabin lights up from the outside and the stewardness shakily tells us to stay in our seats! The pilot comes on the intercom and calmly announces a minor case of "St. Elmo's Fire" (Did I mention that I flew on the 13th and sat in aisle 13? Not that I'm superstitious, mind you.) Eventually we do arrive in Knoxville, and take a limo to the hotel in the pouring rain. We arrive, of course, after the restaurant has closed and there are no restaurants within walking distance. Oh well, peanut butter crackers and soda for dinner weren't too bad except for the funny twinge when chewing.

Next day dawns bright and balmy and the day goes well. Back to the room in preparation for dinner hosted by the organization we're visiting. I had been worrying about that funny spot in my mouth and suddenly discovered a broken tooth! Great, a stranger in town, what should I do? Try the hospital emergency room, I'm told. O.K....that was a mistake, they're no help!

I got the name of a dentist and make an appointment for the next morning. The taxi drops me off at the dentist and I spy a brown dog nestled in the shrubs. "Nice Doggie!" I walk up to the door, turn the handle and the dog attacks! She nipped my leg, tore a small hole in my slacks and scared the life out of me. Finally after what seemed like hours, the dentist appears, calls off the dog, and states, "She hardly ever bites people!" Lucky Me! At least I got a temporary crown for the tooth for next to nothing and a new pair of slacks free.

The rest of the TDY passed fairly uneventfully, but I did have a moment's hesitation when it was time to leave and we were told to board at Gate 13!

OCID: 4009937

TYME SHELL (u)

This is a time shell to compute Greenwich Mean Time (Z) and Local Time based on the System Time. It is written for the IBM PC/XT and ASTW with a color monitor. Shading will be different on USi monitors Pi2 and Pi3. It will not run on terminals with a monochrome monitor.

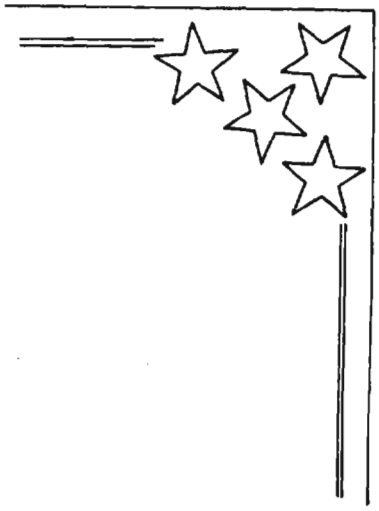
P.L. 86-36

P14

```
echo "\f"                # Clears screen. "\f" is a form feed.                  #
# Set variables $month, $date and $hour.                                       #
month='date "+%m"'          # "+%m" is month portion of system date/time.      #
date='date "+%d"'           # "+%d" is date portion of system date/time.       #
hour='date "+%H"'           # "+%H" is hour portion of system time.            #
   case $month in
          11)     e=S f=05              # Sets EST; $e=S and $f=05.             #
                  ;;
          12)     e=S f=05
                  ;;
          01)     e=S f=05
                  ;;
          02)     e=S f=05
                  ;;
          03)     e=S f=05
                  ;;
          04)     if test $date -ge 28     # Test for last Sunday in April #
                  then e=D f=04        # Sets variables for month of April #
                  else e=S f=05
                  fi
                  ;;
          05)     e=D f=04                    # Sets Daylight Savings Time #
                  ;;
          06)     e=D f=04
                  ;;
          07)     e=D f=04
                  ;;
          08)     e=D f=04
                  ;;
          09)     e=D f=04
                  ;;
          10)     if test $date -ge 27     # Test for last Sun in October #
                  then e=S f=05      # Sets variables for month of October #
                  else e=D f=04
                  fi
                  ;;
   esac                                        # escape case/in test #
   zulu='expr $hour + $f'
echo "\n\t 32m\0311\0715\0715\0715\0715\0715\0715\0715\0715\0715\0715\0715\0715\
0715\0715\0715\0715\0715\0715\0715\0715\0715\0715\
echo "\t 32m\0272\c";date "+     31mTIME:  35m$zulu:%M:%S Zulu     36m(%H:%M E.$
e.T.)"
echo "\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b\b32m\0272"
echo "\t 32m\0272                                                    \0272"
echo "\t 32m\0310\0715\0715\0715\0715\0715\0715\0715\0715\0715\0715\0715\0715\07
15\0715\0715\0715\0715\0715\0715\0715\0715\0715\07
```

```
#  The echo statements above set the colors and draw a box around the      #
#  output when the results are printed on the screen.  Color change        #
#  functions such as 32m are preceeded by ESCC (Escape Key/open bracket).  #
#  Special ASCII characters \0310\0715\0715, etc. are part of the graphics #
#  chara set used to draw a box around the output.  Character constants    #
#  \n, \t, \b and \f are newline, tab, backspaces and formfeed. "\c" kills #
#  the <CR> function.  In /usr/lib/crontab you can replace the statement   #
#  "0 * * * * exec echo "The hour is" 'date'. > /dev/console &" with       #
#  "0 * * * * exec /usr/rej/bin/tyme > /dev/console &" to use your "tyme"  #
#  SHELL rather than the system default time.  Specify the pathname, e.g., #
#  "/usr/rej/bin" to where your executable "tyme" SHELL is located.        #
```

DOCID: 4009937



ON EXCELLENCE (u)

From the keynote address at the Quest for Quality Conference in Seattle in November 1962 by Henry M. Jackson, Senator from Washington.

Published in Achieving Excellence in Public Service, The American Academy of Political and Social Science, Philadelphia, August, 1963.

As never before, we have to provide a government environment that encourages excellence.

Standards of performance adequate for quieter times will not do. State, Defense, the military services, the economic agencies, and the rest of our government must meet new tests of excellence. Yes, and Congress, too.

For two years, our Senate Subcommittee on National Policy Machinery conducted a nonpartisan study of our machinery for making and executing national-security policy. This study had something of a surprise ending: We concluded that the heart of the problem of government is not machinery but men.

Good national policies require both good organization and good people. But people are the critical factor. Wise, experienced, hard-working, incisive government officials may win out over poor organization. But poor people will defeat the best organization.

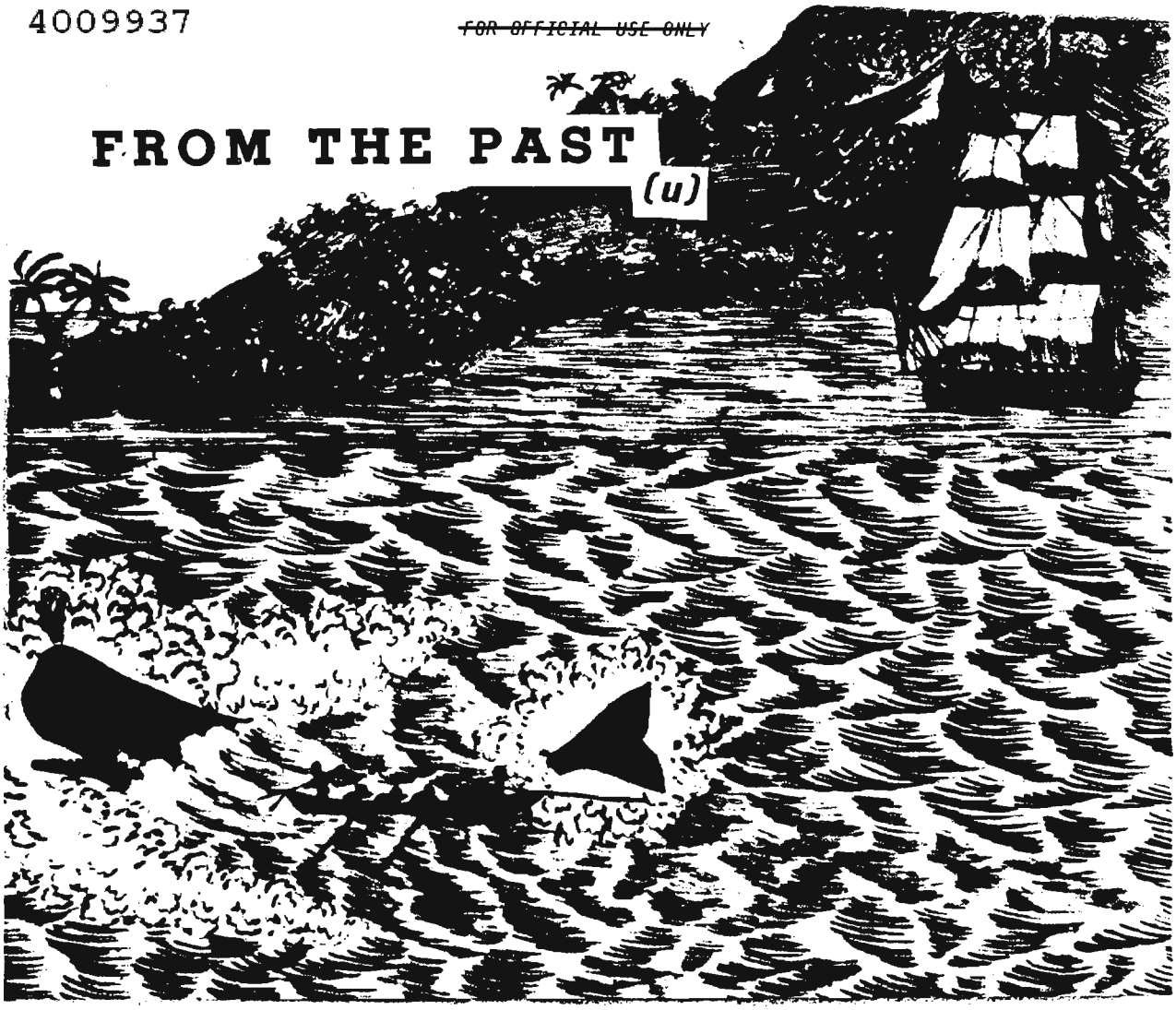
Moreover, reforms in machinery cannot cure troubles which are really not due to defects of machinery. Organizational gimmickry is no substitute for practical measures to improve the competence and the performance of government officials.

Earlier this year, the Senate of the United States established the Subcommittee on National Security Staffing and Operations and asked it to make a study of how well our government is staffed to conduct national security operations.

The Subcommittee's inquiry is based on the simple proposition that the number one task is to get the right men into the right jobs at the right time and to make it possible for them to do a job. Men rise to responsibility, if they are given half a chance. The Subcommittee's modest goal is to help them get half a chance.

OCID: 4009937

FROM THE PAST (u)



The following letter was written by Commodore David D. Porter during the famous cruise of the ESSEX in the War of 1812. The first part is of little interest. Near the end of the letter, however, the Commodore intersperses a bit of cipher.

"U.S. FRIGATE ESSEX AT SEA"

Lat. 2° 26' S, Long. 82° 20' W

July 2, 1813

Excuse me sir for not making known my present intentions as this letter may not reach you, it may however be satisfactory to you to know how I intend to dispose of my prises, let it suffice to say that I shall endeavor to .QD66.94DK.C7.G4C66C.

British letters of Marque are numerous in these seas and were it not for my arrival our whale fishers would have been much harrassed, but they now find it necessary to keep together for mutual protection. I expect to be .AP8QPD2. but shall be .A8DAF8D2.

The State Department will no doubt inform you of the effect our presence has produced; in a .AX6C9CGF6. view on that head I shall be silent.

A British ship shall .7X9.7FØCBF9D.94D.AFGC3CG.C7.QF3D9Q.

To decypher part of this letter I must refer you to the cypher sent me at N Orleans dated 13 June 1809.

I have the honor to be
with great respect
Your Obt Servt,
D.D. Porter

Hon Paul Hamilton
Secy of the Navy
Washington.

OCID: 4009937

~~FOR OFFICIAL USE ONLY~~

NSA-Crostic No. 60

This puzzle, which originally appeared in 1980, has been re-edited to incorporate cryptic definitions. If you need an explanation of these clues, call the Puzzle Editor on 1103s, and you'll be sent one.

Word D, as seen in Word Z

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

84 68 166 255 206 23 179 270 222 103 195 19

273 76 57 148 110 177 123 133 47 263 7

B. If ever I see pond in capital, I'll know

30 39 63 174 143 238 279 159 59 9

C. He, she, you, I, etc., etc., have a low melting point

230 3 244 18 101 207 257 139

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

240 147 12 186 272 226 252 276 210 32 10 40

168 219 108 64

E. New England city trainer warned chimp on chores left undone (3 wds)

176 124 201 278 53 271 13 259 145 202 104 100

107 27 241 161 185 169 88

F. Little junction merges with ease to get rid of undesirables

211 87 105 109 167

G. Rolls follower

138 34 197 77 203

H. Mau Mau stereos are severe and unadorned

60 85 233 116 131 220 162

I. Romantic-sounding town in Florida

122 180 190 72 243 163 130 113 221

J. Richard III sounds quite treacherous

175 80 115 62 196 149 117 208 181

K. My female relative is not Polish civil engineer

141 158 199 89 194

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

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

M. The wheel and tire are to be sent to northern Ethiopia

157 275 260 256 251 78 232

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

24 65 127 223 160 183 29 36

O. Fearful Moro is wearing mixed-up suit

8 277 54 51 97 91 242 135

P. Only the true die well-educated

95 106 155 212 266 69 264

~~FOR OFFICIAL USE ONLY~~

Q. Knockout punch used for storing locomotives

132 235 56 214 182 82 140 38 229 248

R. With time, this is not a waiter

178 164 215 218

S. Toast _____ (3 wds)

258 249 90 21 200 269 137 125 151

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

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

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

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

U. I know why TV blinds five-eyed man of inseparability

268 41 253 58 184 71 142 14 246 216 204 48 20 1

V. Ask Omar Sharif if I can see 1955 robbery movie

193 228 35 111 92 114

W. Totes certain blue terriers?

96 121 154 146 45 26 129

X. Are this lady's jacket and skirt hairy?

94 11 217 156 239 81 187

Y. Headless maid needs help

16 66 209

Z. The only film in which Word D and her husband were co-stars (1959)(4 wds)

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

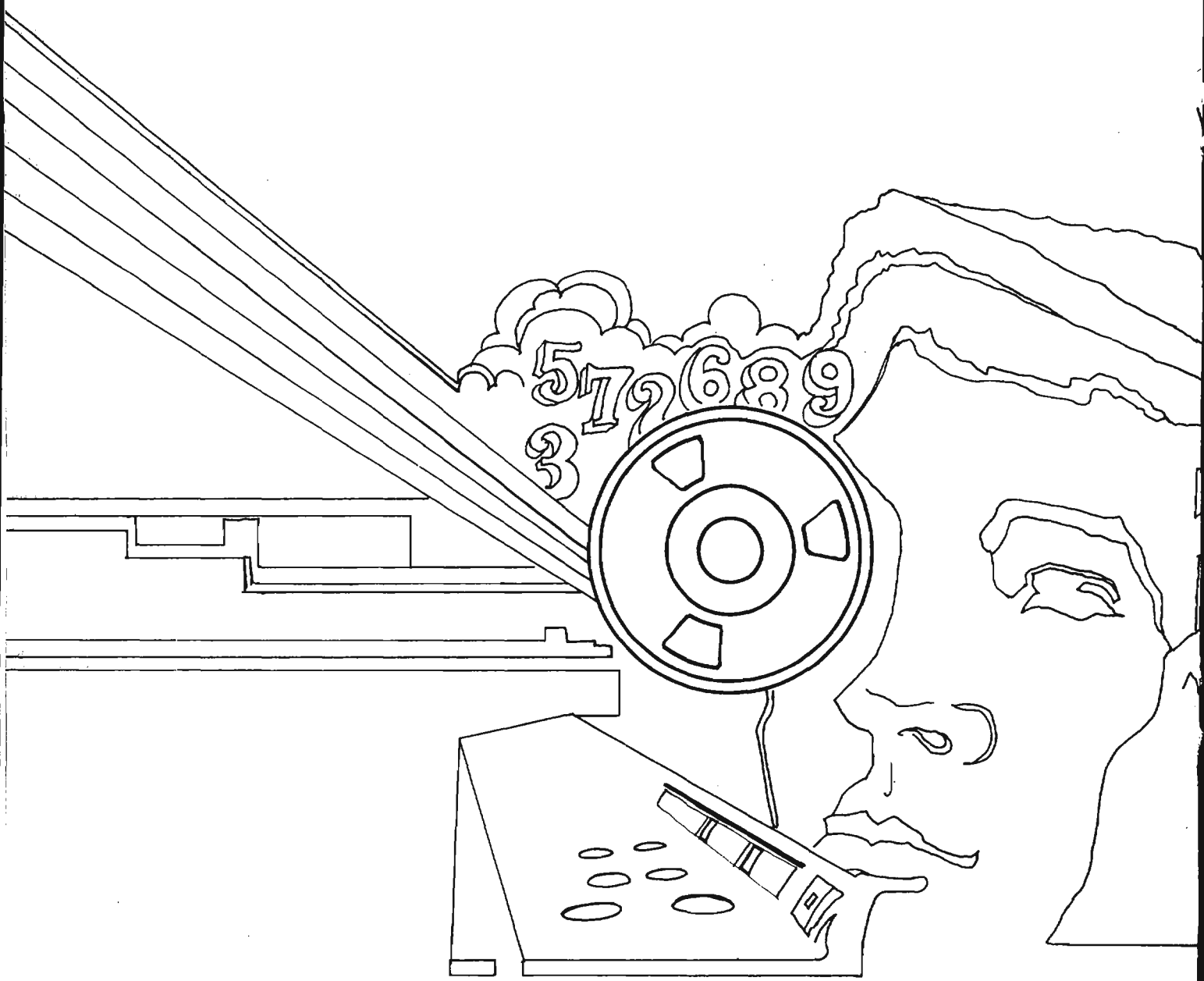
274 49 245 227 170

a. Did you see a emu on going back to New Guinea?

46 153 236 118 172 189

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

P1-May 85-S3-75972


5 7 9 6 8 9
3

This document is from the holdings of:

The National Security Archive

Suite 701, Gelman Library, The George Washington University

2130 H Street, NW, Washington, D.C., 20037

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu