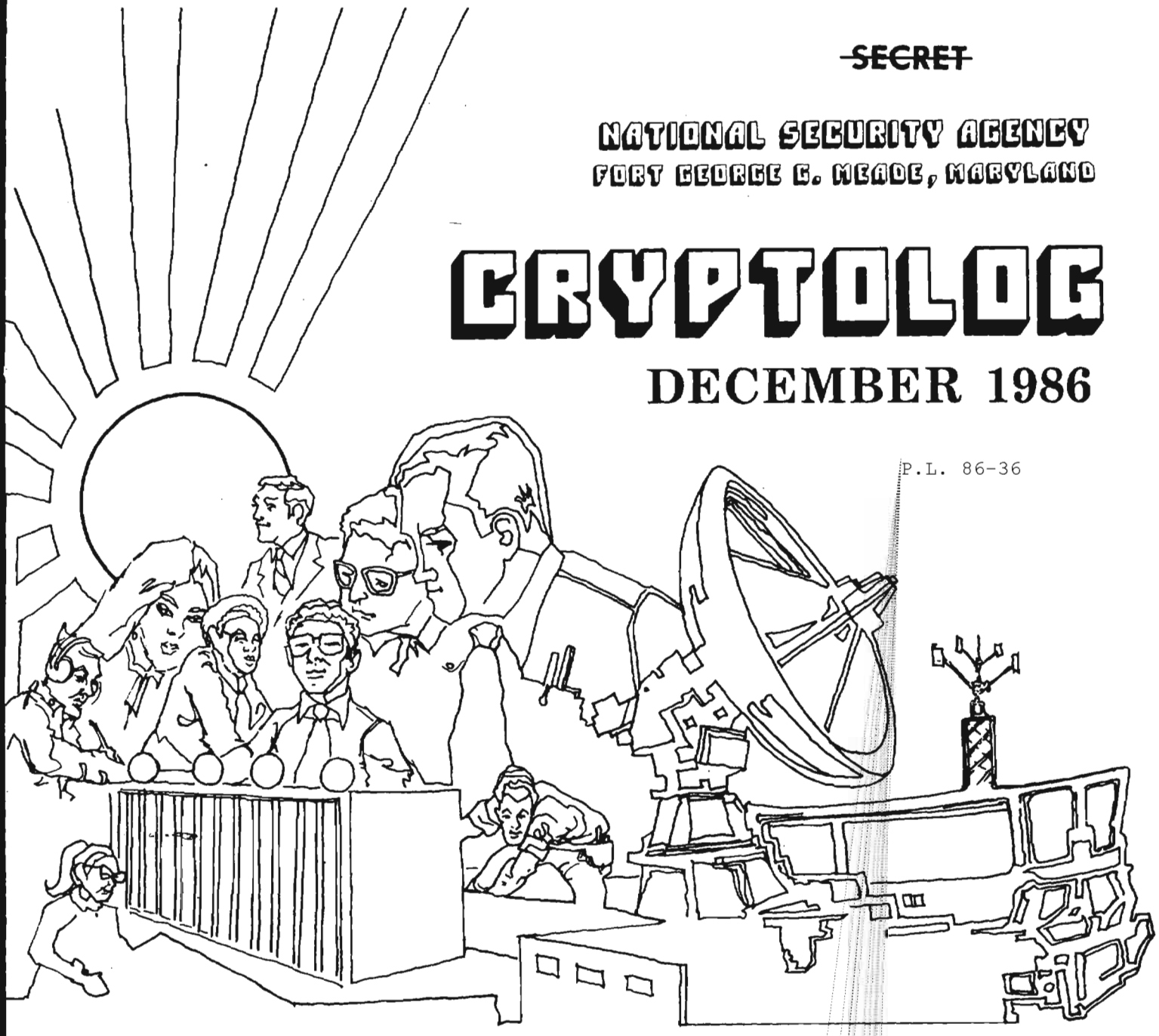
~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

DECEMBER 1986

P.L. 86-36



~~HANDLE VIA COMINT CHANNELS ONLY~~

~~NOT Rreleasable TO CONTRACTORS~~ ~~SECRET~~

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

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XIII, No. 12 ..... December 1986

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

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

via PLATFORM mail, send to:
NOTE CHANGE: **cryptlg** at bar1c05
(bar-one-c-zero-five)
(note: no 'o's in cryptlg)

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

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1 HQ 8A187
Please do not phone.

JULIA CHILD, WHERE ARE YOU? (u)

What this agency needs is a Julia Child to demystify personal computers.

Consider what she did for French haute cuisine: she brought it within the ken of any American who could read.

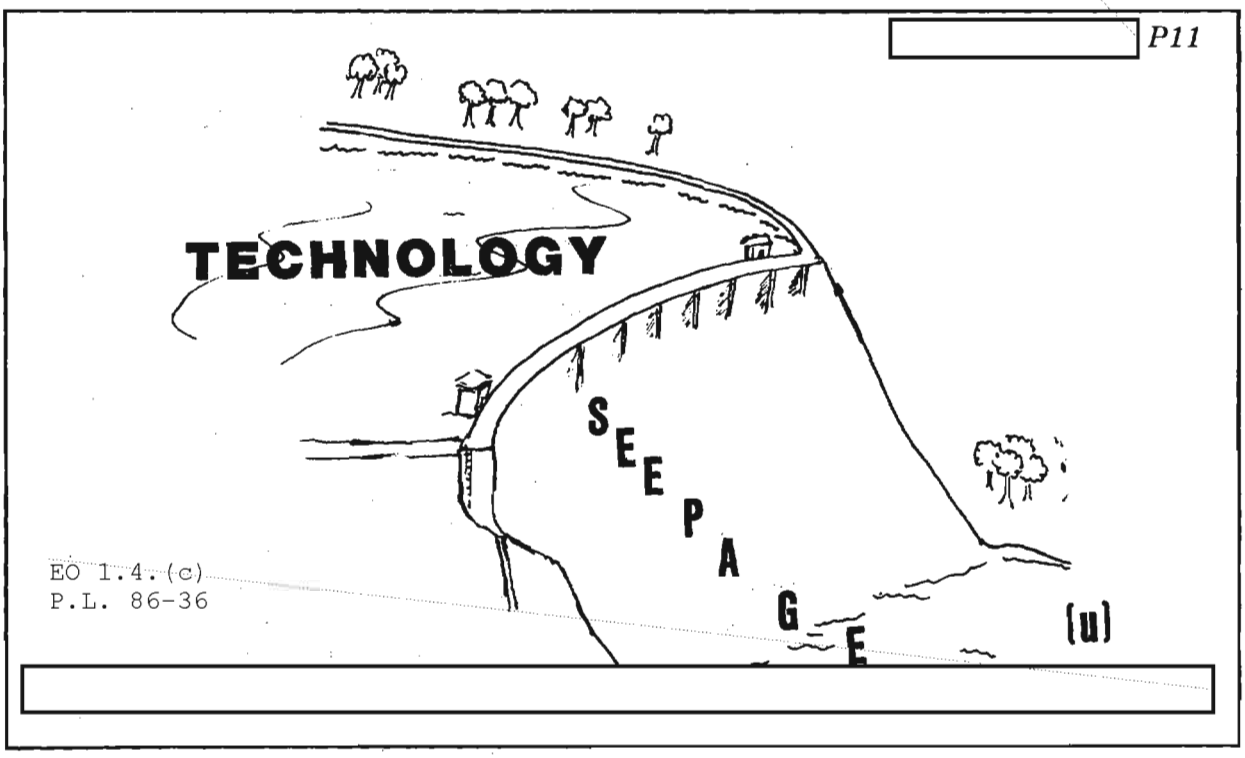
How? Very simply, she wrote a step-by-step handbook with ample illustrations and explanatory notes, all in an informal, joyous, and encouraging tone. Now there's a whole generation who never knew that French haute cuisine was once the exclusive preserve of a select group of the anointed.

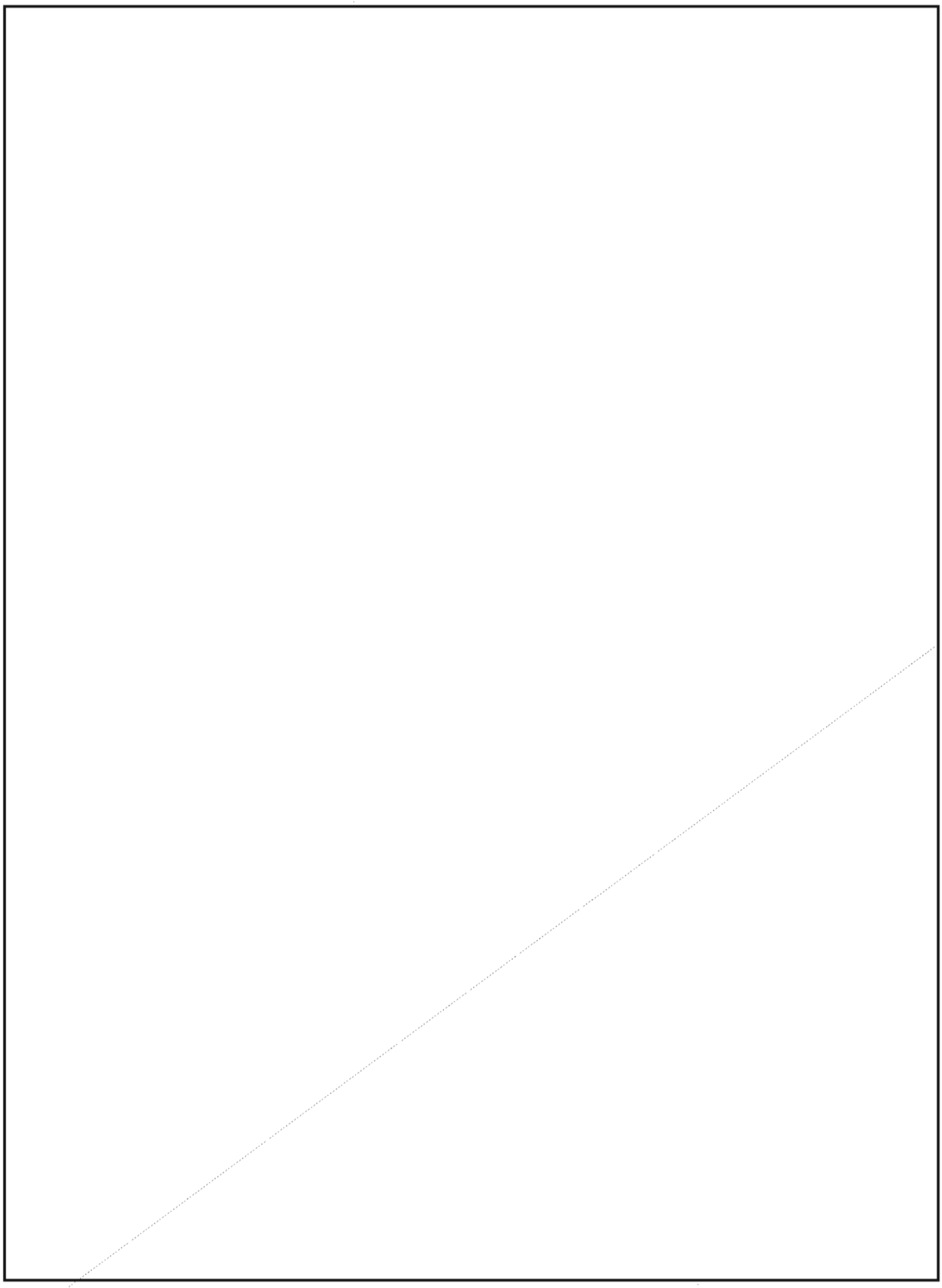
What is odd about personal computers is that they were intended, as the name rather suggests, to be used by anybody. It's not working out that way because the user's manuals are poor. Scan the business pages of the local newspapers some time–you'll see that enterprising people have recognized this and are profiting from it by offering live-in seminars and other courses. And at a price! Highway robbers!

It would be advantageous to develop a handy-dandy for personal computers and maybe software as well, to be issued by the PCIC along with the hardware and software. As it is, many terminals are unused (or underused, solely as word processors) for lack of understandable instructions.

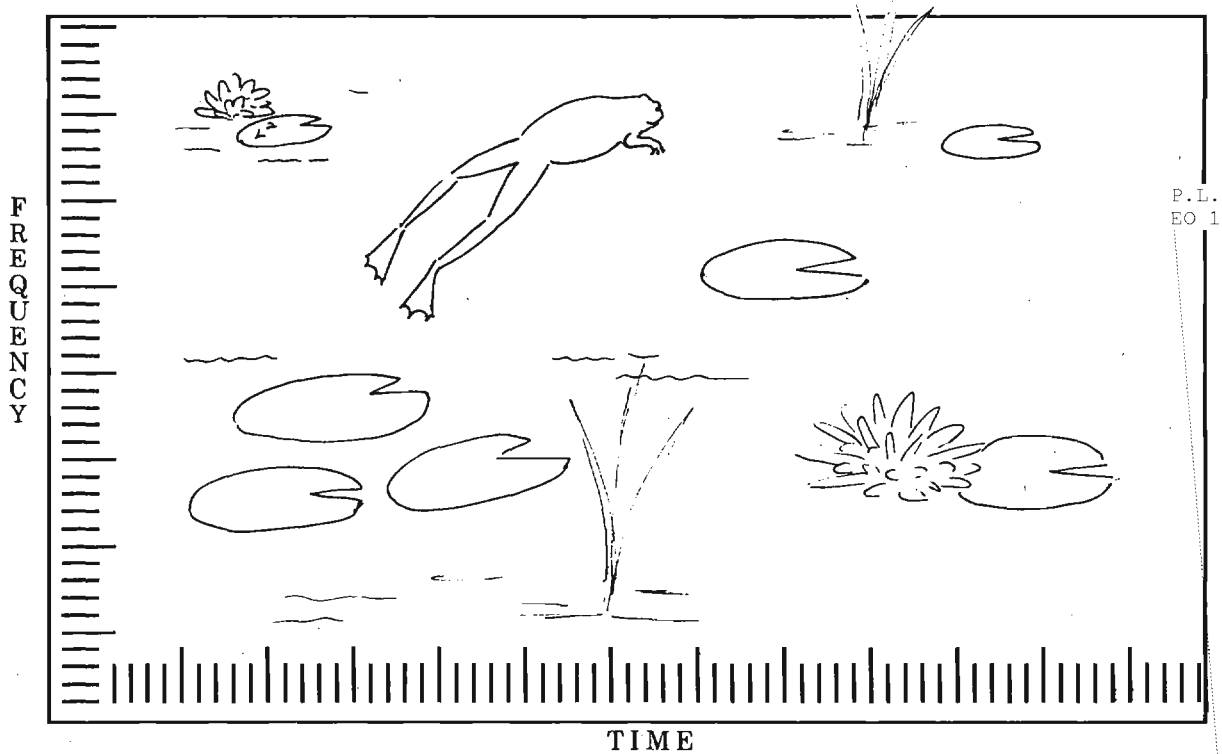
So, in the interest of productivity–think of those hours spent grumbling as well as trying to cope–it behooves Somebody Up There to commission a cookbook-type handbook to personal computers.

And when it's published, please send us a copy.





FREQUENCY HOPPING, VARIABLE DWELL TIMES



spreading code used by the target radio is known, substantially less power is needed to jam its signal. If the spreading code consists of a relatively short recursive sequence, recovery can be made by exhaustive hypothesis testing techniques. Research to develop exhaustive methods of recovering short spreading codes would be unlikely to uncover sensitive algorithms. Longer sequences, such as those above the R20 level, cannot be recovered quickly today by exhaustive testing. To succeed against them, algorithms that parallel those used in extremely sensitive cryptanalytic attacks would have to be developed.

~~(C)~~ The services' requirements are genuine and critical to their mission. They do need a capability to intercept or to jam spread spectrum signals in a tactical environment. There are some who question whether predictive jammers or non-exhaustive spreading code recovery systems are the best - or even viable - ways to provide these capabilities. The services, however, assert that such equipments are vital to fulfilling their mission. And they have the independence, the will, and the money to pursue development.

POLICY ON CONTROLLING RESEARCH

[redacted]

(U) There is no policy that requires the services or other government agencies to coordinate with us before initiating spread spectrum research. Our knowledge of some projects was acquired by chance. We have no way of gauging what portion of the total non-Agency spread spectrum research and development of a cryptologic nature these projects represent. It would take a gigantic, manpower-intensive effort to uncover and track all such projects, and, in the current climate, it would be awkward to do it.

(U) Fortunately, none of the research that has surfaced to date really qualifies as a "smoking gun." But as the number and sophistication of

[redacted]

EXPLANATORY NOTES

Direct sequence spread spectrum signals are those for which the carrier is modulated by a digital code sequence whose bit rate is much higher than that of the information signal. The application of this spreading code spreads the signal across a broad bandwidth. The intended receiver of the signal knows the spreading code and uses that knowledge to collapse the signal back to its orginal form. To intercept or jam the signal effectively, the spreading code must be recovered. The binary streams used to spread the signal can be generated in a number of ways. The use of shift registers is a common method of generating these streams.

Frequency hoppers, as the name suggests, hop from frequency to frequency within a prescribed set. Hopping rates vary from a few hops per minute to many thousands per second. The hopper usually dwells on a frequency for a fixed time but some hoppers with variable dwell times are being produced. A binary stream, generated by methods similar to those used for direct sequence, is used to select the order of frequency use. A specific hopper, for example, might use a table of 256 (2^8) frequencies. It would employ some device, perhaps one or more shift registers, to generate a binary stream. The stream generated by this device would then be broken into 8-bit segments and these segments would be used as pointers into the frequency table. A wide variety of frequency hop radios is being produced, mostly by companies in the U.S., Western Europe, and Japan.

such activities increase, so will the likelihood of serious compromise.

[redacted]

(U) Such a policy statement was drafted and presented to DoD. It was never adopted. The prevailing opinion is that our presentation to DoD was handled awkwardly. This failure to "grease the skids" reduced severely the chances of the policy being accepted. Some people, however, believe that no matter how well it had been presented, prospects for adoption of the policy were slim. The military services are certain to view such a policy as an attempt to invade their domains, and they are zealous and effective in protecting what they deem to be their turf.

[redacted]

options. For example, pursuing Option 2 would not preclude some of the research from being done at NSA. If Option 3 were chosen, some of the research and development might be contracted by NSA to industry or the academic community.

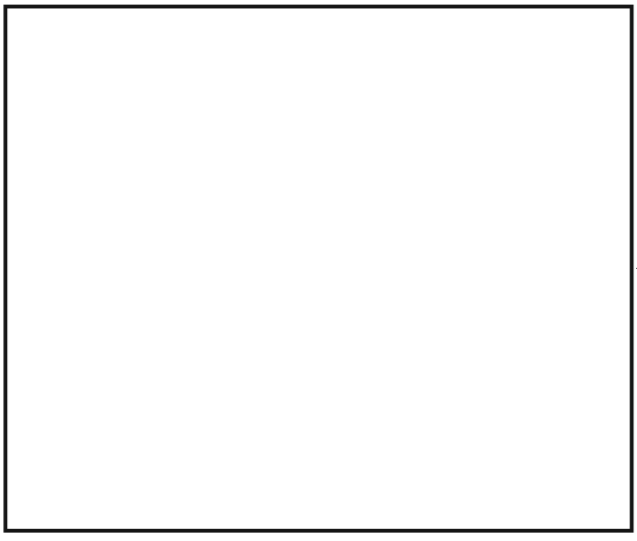
Option 1: Case-by-Case Problem Management

(U) This is the option we have pursued so far. When incidents of outside research and development in this area are discovered, the particular circumstances of the case are evaluated and an appropriate course of action is selected.

Advantages

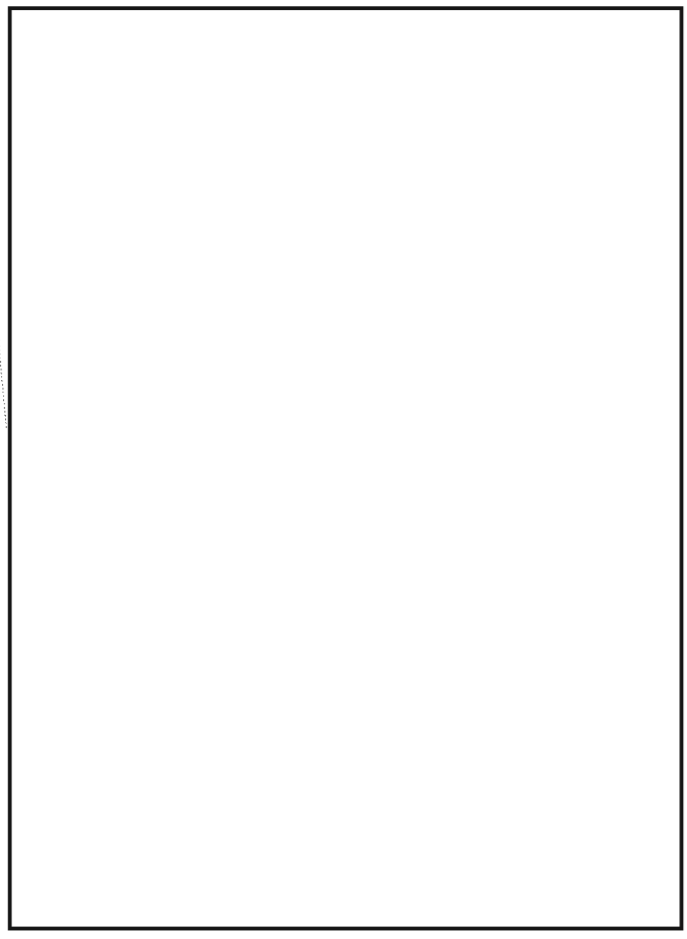
(U) So far, we have been able to resolve all the cases brought to our attention in a way that is reasonably satisfactory to all concerned.

(U) The services are rightfully jealous of their prerogatives. While they might see actions taken under this option as intruding on their turf, they might find them more acceptable than the systematic intrusion that would be introduced under Options 2 and 3.



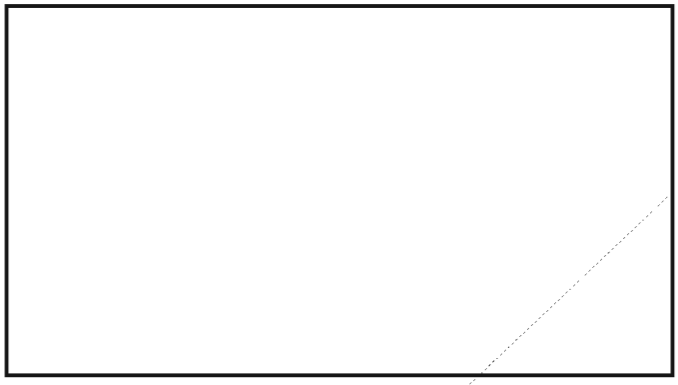
Disadvantages

(U) This option depends upon controlling by persuasion that which is discovered by chance. It provides no systematic way to find out what research is being initiated and, despite our success so far, there is no assurance that we will be able to influence that which we do discover.



(U) As a first step in implementing this option, DoD would have to require that all government-sponsored research and development on spread spectrum be coordinated with NSA. A monitoring system based upon voluntary compliance would have little chance of succeeding.

Advantages:



(U) While the monitoring mechanisms required by this option would make this option more expensive than Option 1, it would be cheaper

than Option 3. It would also require fewer people with critical skills than Option 3.

Disadvantages:

(U) Little could be done to implement this option until a DoD policy requiring coordination with NSA on spread spectrum projects was adopted. The risk that we could *not* obtain such a policy is high. Even if we succeed, a great deal of time is likely to pass before the policy is adopted and promulgated. Changing DoD policy is a slow, tedious business.

[redacted]

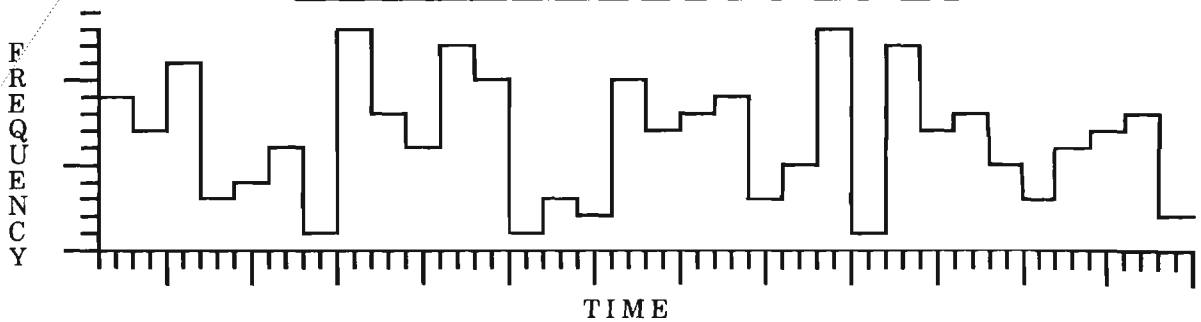
(U) The services would view implementation of this option as an intrusion into matters that have been, and in their view ought to continue to be, within their jurisdiction. They could be expected to resist both the regulation and any control mechanisms we established. It would be difficult to write a proposed DoD regulation so that the bounds of our authority were clearly defined. The services would likely seize upon any ambiguity in it to justify not coordinating with us or disregarding our counsel.

[redacted]

[redacted]

~~(C)~~ COMSEC regulations, policies, procedures and programs might be used as a model for a

FREQUENCY HOPPING, FIXED DWELL TIMES



system to control the deployment, accounting, use, and maintenance of spread spectrum equipment containing sensitive components.

Advantages:

(U) NSA's active role under Option 3 would provide much greater control over the technology seepage problem than would the Agency's passive participation under the other two options.

[redacted]

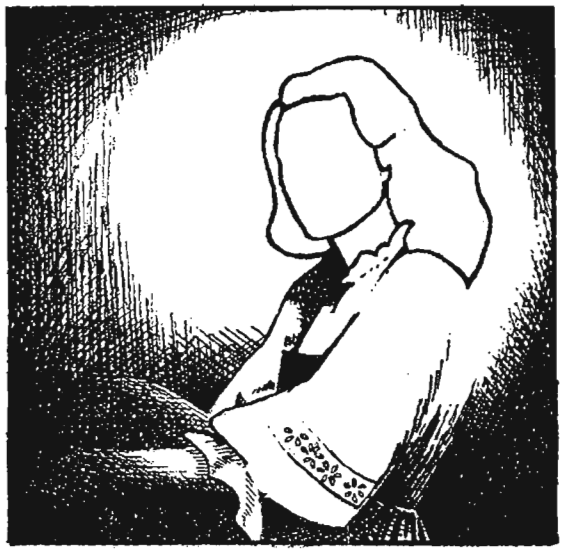
(U) Under either of the other options, it would be difficult to control duplication of research and development by the individual services and by us. By accepting responsibility for the sensitive components, we would not only ensure that the research and development for them was done securely but also that it was done without expensive duplication.

(U) Protecting sensitive techniques during the research and development stage is just the beginning. Safeguards must be applied to all facets of the product's life cycle. Care must be exercised in how the system is deployed, accounted, used, and maintained. Under Options 1 and 2, it would be difficult to persuade the services to institute life-cycle control procedures that would provide a sufficient level of protection for sensitive components. Those life cycle support control procedures that were employed probably would

[redacted]

(U) Openness would not mean disclosing fully everything that we are capable of doing. It would, however, require us to explain to the services what we can do, what we can't do, and that there may be some things that we can do but cannot provide to them. We would also have to provide an acceptable rationale for not sharing some capabilities with them. We believe that our decisions on what to release will be based upon sound technical judgments. We should be able to convince the services that they will not be made arbitrarily or out of contempt for their capabilities.

(U) There are no easy solutions to this problem. Option 3, if implemented well, would minimize the risk of disclosure of sensitive cryptanalytic techniques at all stages, from initial research to field operation of a system.



WHO IS SHE?

P.L. 86-36

[redacted] *T54*

She was born Hedwig Eva Maria Kiesler in Vienna, Austria, the only child of a prominent banker. In 1938, alarmed at the growing threat of Hitler and the Nazis, she left her native land and came to America, where she became one of Hollywood's most glamorous stars.

Her fans never suspected that she was also playing another role, that of inventor. In 1942, composer George Antheil and H. K. Markey (her married name) were granted a patent on their "Secret Communication System," a way of guiding torpedoes to their targets by frequency-hopping, spread-spectrum radio transmissions. A technique nearly identical to theirs was later used operationally by the U.S. Navy.

Who is this actress-inventor?

Answer on page 20.

Note Change in Electronic Mail Address

c r y p t l g @ b a r l c 0 5

no 'o'

CRYSCO - 87

FOURTH ANNUAL CONFERENCE

8-12 June 1987 at NSA

Sessions held in the Friedman Auditorium and in Conference Room 2W087

AUDITORIUM SESSIONS ARE OPEN
to persons with a green or orange badge

OTHER SESSIONS REQUIRE TICKETS
(distributed through your office)
a green or orange badge
and LACONIC access

★

General topics include:

- CRYSCOs in review;
- IDA/CRD and IDA/SRC updates;
- UNIX conversions;
- Transition to UNIX;
- Future workstations;
- Mass storage requirements and proposed solutions;
- Supercomputing trends;
- Programming multiple CPU and massively parallel systems;
- Requirements for software management system;
- Computer graphics;
- IOSP updates;
- Software development standards: do they work?
- Reports from CSE, DSD, and GCHQ;
- OWL libraries;
- CRYSCO-87 wrap-up.

★

Additional information can be obtained from the CRYSCOM executive, [redacted] *A538/P13, 963-4196.*

~~(FOUO)~~

P.L. 86-36

QUOTE WITHOUT COMMENT

Editor's Note: A number of readers sent us copies of the following translated excerpts from an article that appeared on 25 March 1986 in a literary magazine of the United Emirates Republic.

"

¶ Only a few people know that this agency actually exists; almost no one outside the US knows anything about it, while one out of a hundred thousand Americans knows of its existence.

¶ The annual budget of the NSA is $12 billion, and it employs sixty thousand Americans.

¶ Its chief assignment is to know everything, not only inside the US but everywhere in the world. It traces all telephone and radio calls whether their subjects are political, military, economic, cultural or even personal.

¶ It possesses almost absolute power; its ears and eyes are planted everywhere, but mainly in the Soviet Union. NSA personnel were the first to know of the crash of the Russian space shuttle, Soyuz.

¶ Its equipment and staff are able to analyze ciphers.

¶ It is not an exaggeration if we say that if Gorbachev sneezes the White House will be the first to hear it.

¶ The agency was established in 1952 during the second term of former president Truman. It is not subject to the oversight of the congress or any other US organization. Furthermore, it does not legally exist. When it was established, only the president and national security advisor knew about it.

¶ The NSA headquarters is located inside a thick forest of cedar trees near Fort Meade, Maryland, two hundred kilometers from Washington. The complex is very well protected and is more or less a fort, equipped with the most advanced electronic warning systems.

¶ The staff are chosen from among the personnel of other security agencies after being subjected to psychological training courses and a detailed scrutiny of their personal files. Because wives love to gossip, only bachelors are allowed to join the NSA. The staff may only marry each other.

¶ The staff is only allowed to have the minimum amount of social relations or may not have any social life at all.

¶ The NSA has very advanced computers, one for analyzing normal calls, and the other to pick up and analyze coded calls. The average number of calls that the computers receive daily is 300,000 normal calls and 200,000 enciphered calls. These computers are able to read and to analyze codes at up to 600 lines per minute and in all languages.

¶ The agency is a field study' of the most up-to-date scientific advances.

¶ Like the human brain, the agency's brain' is divided into two parts. The right part, named CARION,' is equipped with four linked IBM 3033 computers attached to three huge printers that are able to print 22 thousand lines a minute. The left part is equipped with super computers each of which weighs 5,000 kilograms and are able to do 200 million operations per second. NSA computers write up to 320 million words per second.

¶ Outside the USA, the agency has secret operations branches in Japan, Taiwan, South Korea, West Germany, South Africa, Lebanon and Turkey. These offices are usually described as annex buildings to American embassies, consulates, and US cultural and commercial organizations.

¶ The agency relies mainly on satellites that are specialized in espionage. From an altitude of 200 kilometers, these satellites are able to photograph any object that is two feet or more above the surface of the ground.

¶ The reason some of the NSA's secrets are being revealed at this time is to preserve part of America's image of technological superiority which was injured after the CHALLENGER tragedy. □

"

The Language Identification Problem (u)

P16

P.L. 86-36

~~(C)~~ A message in a language that no one can recognize is a vexatious thing: there is no knowing whether the information is trivial or important as long as the text cannot be understood. Even if the information in itself is not valuable, there is the possibility that identifying the language may be helpful for making decisions and adjustments in collection.

~~(S-CCO)~~ The first thing we have to do is to get rid of the idea that language identification is simple. Language identification is a large subject that has only begun to be explored along lines that we would find useful. To begin with, consider the problems:

- The way in which language recognition takes place is not well understood. It appears that all people do not do it the same way: some rely principally on recognizing individual words, and others primarily on recognizing rhythm, cadence, and overall effect.

- Estimates of the number of languages in the world have run mostly between 3000 and 4000, and have tended to keep rising. The number of languages in Africa is said to be at least 850; in India, 800; in the USSR, 130; in South America (with less certainty) perhaps 500 or more, and so on.

- In the future we can expect to get more intercepts in unidentified languages than before. This will be due to increasing international travel and commerce; the use of foreign labor; the growing availability of radiotelephone, satellite communications, and multiple channels; and new collection techniques with more comprehensive intake.

~~(FOUO)~~ Fortunately for us, while 4000 is a meaningful figure in the field of anthropology, in the world of communications it is not. In practice, we are not going to have to identify 4000 languages. The vast majority are minor languages, spoken in remote and primitive areas and by tiny populations, some of them in single villages and 30-person tribes.

(U) Of the 4000 languages, about 100 are spoken by 3 million people or more, and another 50 or so are spoken by 1 or 2 million; all the rest have fewer than a million speakers apiece. Only about 70 languages are official languages of a national government. (This is because Arabic, English, French, and Spanish are used by so many. The number of countries in the world is about 170.) Another 15 or so are languages of sizable and well-known minorities.

~~(C)~~ In real life, we are going to find ourselves dealing with the same languages most of the time, and there will not be much more than

100 of them, which is still enough to give everybody plenty to do. My own experiences have generally fitted in with this principle: When it is an official national language, we can usually identify it; when it is a well known minority language, we have a good chance; and when it is neither of these, it can become very hard going.

[redacted]

~~(C)~~ How do we deal with all this? Experience has brought some pieces of accumulated wisdom with respect to both voice and graphic communications, as well as a subset of the latter, handwriting, which must be considered separately.

~~(C)~~ The ideas I present below are based on my own experiences with language identification. These ideas are set forth as suggestions for linguists and ways that managers and supervisors can help.

I. POINTERS FOR LINGUISTS

~~(FOUO)~~ Following are some suggestions for linguists who have been tasked with identifying an unknown language. Voice communications, message traffic (often referred to as "graphic"), and handwritten material are each considered separately.

A. VOICE COMMUNICATIONS

Try Rewind.

~~(FOUO)~~ Probably the first thing to do with a voice tape that defies identification is to try running it the other way, in case it has not been rewound. Don't laugh: a remarkable number of unidentified languages have turned out to be Russian or English in reverse.

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

Look for a short speech segment of one or two syllables or words.

(U) Often the easiest way to identify the language of a conversation by word recognition is to concentrate on the shortest speeches in the exchange. Short speeches by nature present the fewest word division problems, tend strongly to stereotyping and the use of common words, and usually represent simple ideas.

(U) The three primary short speeches are **Yes, No**, and **What?** A highly favorable case occurs when there is a long speech of one or more sentences, a short response of only a syllable or two, and then a repetition of the long speech. The odds are that the short speech means **What?**. Or if the response is longer than one or two syllables, it is likely to be: **"How's that?" "What did you say?", "What was that?", "I didn't get that"** or **"I couldn't hear you."**

(U) Now you will find it much easier to check for a word or phrase in dictionaries or lists when you know what you are looking for. (Unfortunately, there are people everywhere in the world who say "Aahh?" or "Haahh?" instead of "What?")

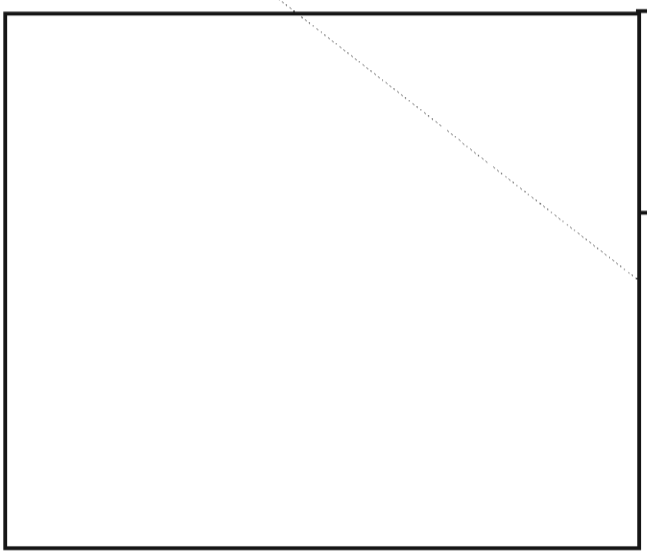
Keep an Open Mind, and Try Again.

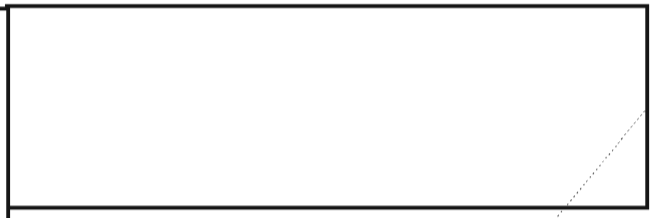
[redacted]

Consider the possibility of intrusive foreign words.

(U) International word borrowings "contaminate" language samples and have a cluttering effect that makes identification harder. Words of international scientific and

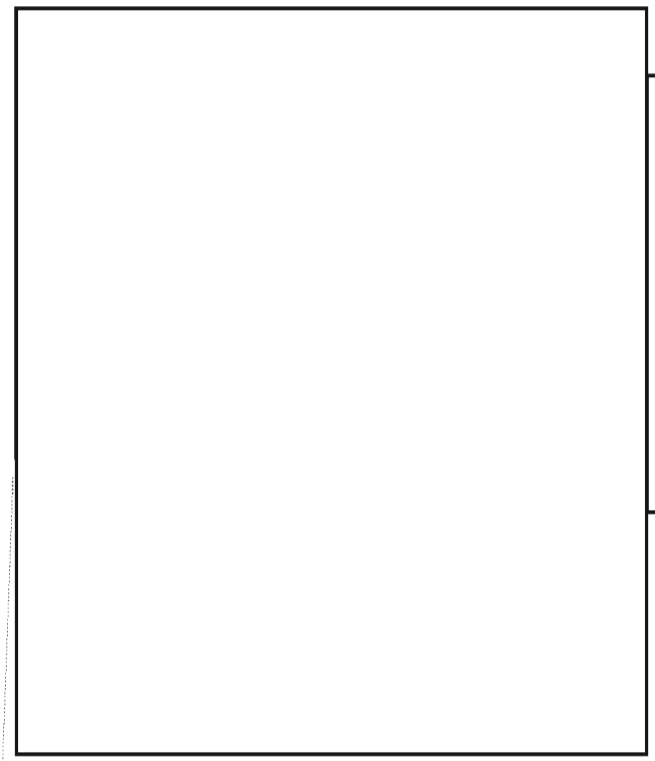
EO 1.4.(c)
P.L. 86-36





technological vocabulary like "telephone" are so widely adopted that they only hinder identification.

(U) Languages of Islamic countries have a considerable stock of borrowed Arabic words, and frequently it is the same Arabic words that several unrelated languages have borrowed. Obvious examples are Persian (Indo-european), Uzbek (Turkic), and Indonesian (Austronesian), which have many of the same Arabic words in common.



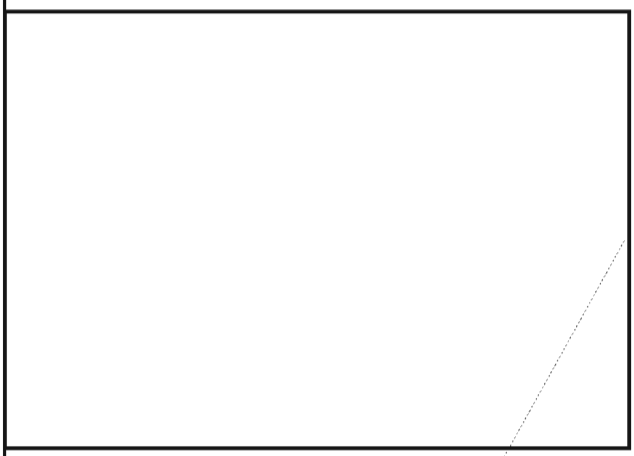
Establish What is Good Text by Finding Repeats.

(U) Make a photocopy of the text so that you can mark it. Then underline every string of letters that occurs in the text more than once. This will usually ensure that the things you are looking for in dictionaries are not garbles.

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

Collect References

(U) There are several identification books, intended for librarians and printers, which devote a page or two to each language and give a paragraph of sample text. Some of them also give some information about the grammar and point out some common words that are characteristic. One drawback is that the sample paragraphs are quite short and often fail to include some very characteristic words. Another is that the samples are given as they would appear in a printed book, whereas traffic is often in transliterated form, and there can be several transliteration systems for the same language.



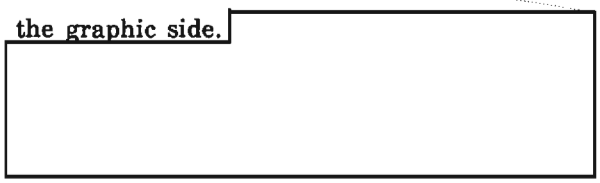
C. HANDWRITTEN MATERIAL

~~(FOUO)~~ Handwritten materials present special problems and must be considered separately. Generally, they present the hardest problems on

P.L. 86-36

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

the graphic side.



(U) Handwriting that can be matched to a known cursive script, such as Arabic, Russian, Greek, Armenian, Georgian, or old Albanian is easily identified. Samples of cursive writing can be found in the following books. Call numbers are those of the NSA library:

Diringer, D: *The Alphabet.* 1968. P211.D62.1968 (2 vols)

Jensen, H: *Sign, Symbol and Script.* 1969. P211.J45gE.1969

Hoskins & Meredith-Owens: *A Handbook of Asian Scripts.* P213.B77

(U) What is not easily identified is handwriting with partial resemblances to one or more known scripts, especially when the characters are connected to each other, creating great uncertainties about how to separate them. Handwritten pieces of this kind present too many questions all at once: Is it plain language in an unidentified language? Is it really writing at all, or just doodling? Or done by someone under the influence of a narcotic who thought he was writing? Or a hoax? If it is plain language, why can't we match it with a known script? Is it a cipher? If so, we are at a great disadvantage in not knowing what the underlying language is, and at another great disadvantage in not knowing how many characters there are and what they are.

(U) For example, if we were looking at an unknown script that contained signs like English handwritten c and cc, e and ee, l and ll, t and tt, all letters made with only one or two strokes, we could not be sure whether cc, ee, ll, and tt were connected double letters or separate letters in themselves.

(U) Again, we can start by looking for repeated sequences, which would suggest that the text was not random doodling (but would not prove that it was not), and for repeated combinations followed by spaces, which would suggest grammatical endings in an inflected language, either in plaintext or in simple substitution. After that we are in for a long effort with poor prospects.

~~(FOUO)~~ Among the many problems are the alphabets, sometimes bizarre, that are invented by the writers; fortunately, these often prove to be monoalphabetic substitutions of a well-known language, and so they are easily solved. An important diagnostic feature of invented alphabets is that the characters are usually clearly drawn and clearly separated.

~~(FOUO)~~ An example of all of these problems is the Voynich manuscript, a unique European manuscript thought to date most probably from the 15th or 16th century, which has resisted solution, not only by philologists early in this century, but by NSA cryptanalysts as well.

II. HOW MANAGERS CAN HELP

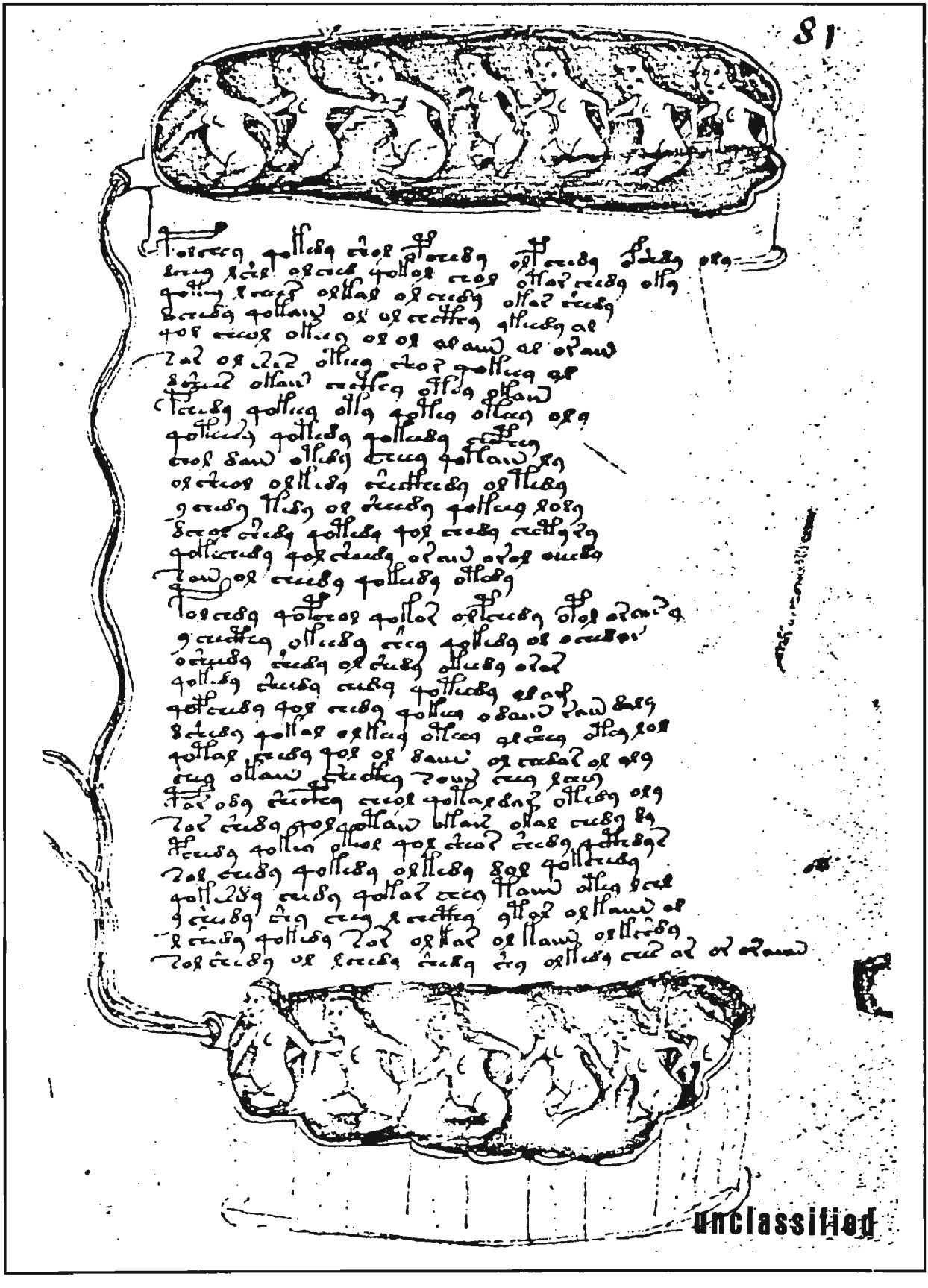
~~(C)~~ Simply having a list of expert voice linguists who can be consulted has been tried; it was found that the list required constant updating because of normal employee turnover. In any case, the old practice of carrying a tape around and trying it on various linguists is slow, inconvenient, unreliable, and not always successful either. It is also heavily dependent on luck and guesswork in finding the right linguists to ask.

(U) But there are several other ideas that might be tried to improve our success rate in identifying unknown written text. And these depend upon the active support of managers and supervisors.

~~(C)~~ Messages in unidentified languages turn up only sporadically but persistently. Because they constitute a recurrent problem but not a continuous one, they are dealt with individually, without any method or system and without any record of what was done and what resulted. They should be dealt with more methodically. What I have in mind would not involve concentrating and centralizing identification efforts but would be the opposite of that: making more analysts able to do identification by providing information on it

~~SECRET~~

THE VOYNICH MANUSCRIPT (u)



unclassified

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

more systematically. By no means are all of these new ideas.

(U) In general, supervisors and managers can do two things to help linguists identify unknown languages:

Support the Development of a Training course.

~~(FOUO)~~ Training is not a new idea. It would have the advantages of introducing methods in a package, rather than have everyone rediscover them individually, of furnishing supervised familiarization and practice, and of providing a basis for the creation and distribution of working aids. For example, the course could include a brief and practical introduction to phonetics, with special attention to speech sounds in a wide variety of languages.

Provide Reference materials.

(U) Recognition is by nature matching. The analyst must be provided with bases for comparison. This may mean purchasing books, subscribing to periodicals, and acquiring video and other voice tapes.

(U) Now for some specific suggestions about each type of language identifcation problem.

FOR VOICE TRAFFIC

Encourage the Use of the Tape Library.

[redacted]

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

Support the Updating and Expansion of Existing Word Lists.

[redacted]

Commission the Compilation of a Word Grid.

[redacted]

FOR A WORD GRID

Yes, No, What?
Hello, Hi, Goodbye, So long
Thank you
Wait a minute
Who is calling?
All right, Okay
That's right
I understand, I see
Listen, ...
Don't hang up!
That doesn't make any difference
Fine, Excellent
Impossible
Immediately
Necessary
Important
Will arrive
Because
North, East, South, West
Yesterday, Today, Tomorrow, Tonight .
Day, Night, Week, Month, Year
Next, Last (Week, etc.)
Names of weekdays
Names of months
Numbers from 1 to 10
Selected higher numbers, e.g. 100, 1000

P.L. 86-36

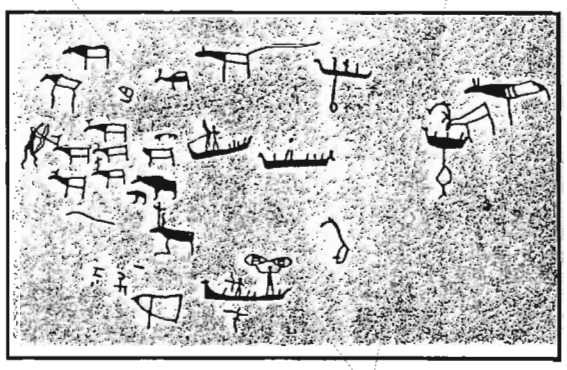
amount of text and without "too many" borrowed or foreign words.

Collect Samples of Transliterations and Romanizations.

~~(S-CCO)~~ Printed books on languages regularly give each language in its traditional writing system.

Sponsor In-house Research.

(U) Possibly some of the many things that are not known in language identification could be resolved by study and investigation. For example, there appears to be a difference of opinion on whether it is possible for someone who doesn't know a tonal language to tell whether it is one merely by listening to it. The objection is that in at least some cases it may be difficult to tell word-intonation from sentence-intonation. If this question could be settled, it would be a valuable piece of information in language identification.



P.L. 86-36

A FINAL WORD

(U) There is a great deal to be done in language recognition. At this time no one knows how many possible approaches there are, and no one system can claim to be invariably successful. □

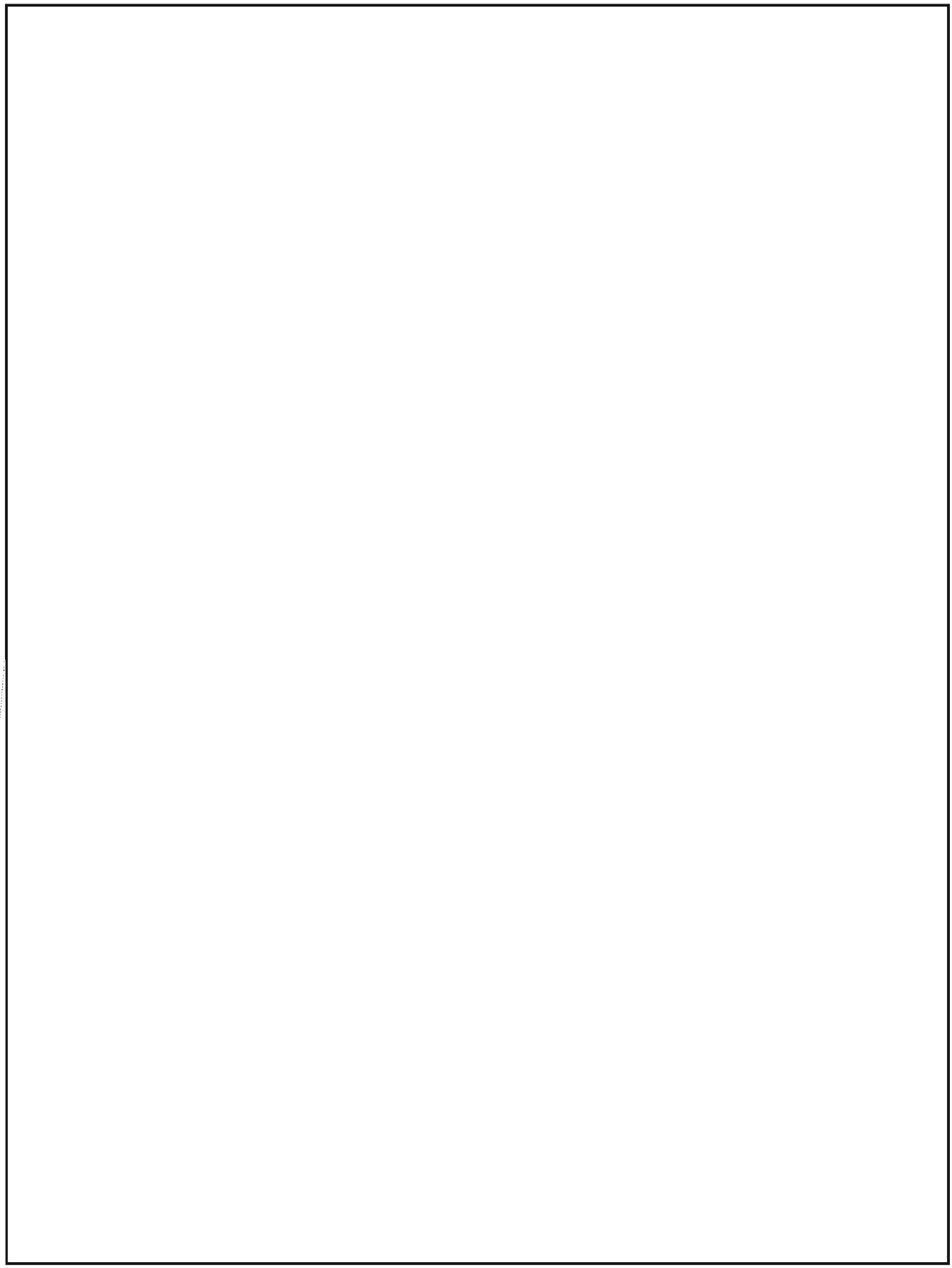
PRODUCT vs. PROCESS: One View (U)

[redacted] G14

~~(FOUO)~~ Like the management of many other middle-aged organizations, the management of NSA is forgetting why the organization was created. The auxiliary functions of the Agency are distracting us from our primary task of producing intelligence information. In other words, we have become enamored with the process at the expense of the product. Recognition of this situation is critical because there is no "bottom line" to measure NSA's effectiveness; there is no danger signal to alert us that all is not well. (Some may argue that customer satisfaction is the "bottom line," but I believe that the customer is not aware of what could be provided and, therefore, makes decisions regarding NSA product without knowledge of our full capabilities.)

[redacted]

[redacted]

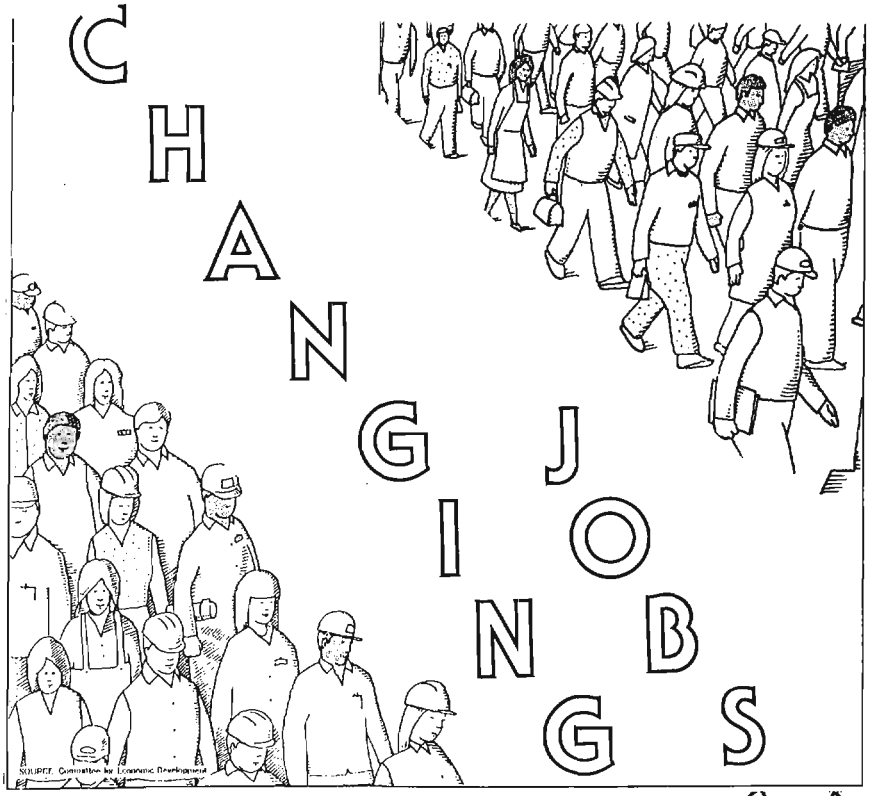


P.L. 86-36
EO 1.4.(c)

Answer to **WHO IS SHE ?** *on page 10.*

Hedy Lamarr, who once said, "Improving things comes naturally to me."

CHANGING JOBS (U)



P.L. 86-36

g221

So you want to change jobs within the Agency? One of the great advantages of working at NSA is the vast array of varied opportunities awaiting you. Unfortunately, many employees find it difficult to move. It doesn't have to be.

The first step is to determine your goals. For some the goal is to become a senior executive, while for others it is the more modest goals of enjoying their jobs and receiving reasonable promotions. Some employees want to work within a particular discipline and move around among different targets, and others are enamored of a particular country but want to work on various aspects of that target; still others want to diversify, and seek assignments in other fields such as personnel, logistics, COMSEC, etc.. And then, of course, there is the question of management or tech track. Once you have examined your personal needs and determined your goals you can start looking.

In order to be able to move easily you must first establish yourself as a skilled and willing worker. Get your assigned tasks completed and then ask your co-workers to teach you what they are doing. Ask your supervisor to give you tasks outside your normal range of duties. Learn everything you can. Take every course in your discipline that you can arrange. There are self-study courses in abundance, and you may find a learning center open after or before your normal duty hours. Try changing jobs within your current organization; that's generally an easy move.

Once you have established yourself as a skilled, experienced, and willing worker, start the above process in reverse. Teach your skills to others in your office; train someone to do

your job or train several people to do different parts of your job. The mission, your co-workers, and your supervisor all benefit from this approach, and so do you. This course of action will allow you to move, for it is often easier for managers to find and hire someone at a lower grade. Don't fall into the trap of trying to make yourself indispensable; if you succeed you are doomed to stay in that job.

Write a complete and detailed description of your job. No one is more capable of doing this than the individual doing the job. This has multiple benefits. Not only will you surprise yourself (pleasantly) in finding how complex your job is, but by detailing it you may think of some ways to broaden or simplify the tasks or to improve on your performance. The description will also serve as a detailed guide for your replacement for learning your duties. In addition, your supervisor will be able to use this job description when writing your performance appraisal as well as a guide to writing a vacancy announcement, and even as a tool for interviewing applicants for your job.

Use your network of friends and acquaintances to look for a possible successor. Even if your job is all wrong for you, you may know someone else who would be a perfect match for your job. Suggest they come and talk with your boss. In fact, everytime you hear of someone looking for a job change or hear of a job opening, try to help.

All this, and we still haven't gotten around to discussing how you are going to find a new job! Well, being in a position to be granted a release from your present job is the first step in moving. Without it, you will have to find an advertised job, and even then, your supervisor can hold you for 90 days. Obviously, one of the secrets to moving is making it easy for your supervisor to let you go.

OK, now you are ready to move. How do you find that new job? My first suggestion is to review your goals, looking for various intermediate paths to achieving your goal. You can stay in one place a long time waiting for that one "perfect" job or you can be flexible and take a series of jobs, all of which teach you new things and allow you to make various contributions.

Now start talking to the people in your network. Of course you have one. They are the folks you eat lunch with, members of any Agency clubs you belong to, people you deal with professionally in other offices. If you've been trying to help them, they'll help you. Find offices which interest you and make an appointment to talk to a branch or division chief in that office. Ask your boss to check out his or her network for openings. Go to your Pers Rep and your Career Panel Exec and let them know you are looking. Don't assume that all advertised jobs are bummers. Talk to anyone who has a job which might in anyway move you closer to your goal. The job might not have the "right" title but the duties may be exactly what you are looking for, or close enough to fill the bill. Remember that you can apply for a job one grade above or below your current grade. (No, you don't take a salary cut.)

Get your Personnel Summary in tip top shape and have copies available. Make sure you have neither under nor over- sold yourself. Find ciritical friends to review it for you. Ask former supervisors if you can use them as references. If you are a GG-12 through GG-15 make sure that the SPCP folks (M44) are aware you want to move. Be creative, innovative, even daring in looking for ways to promote your job search. A large portion of Agency jobs are constantly being vacated, and the opportunities are there waiting for you.

Having found some interesting openings, interviewing for the position is the most important thing you can do. Many (even most!) NSA supervisors have never been trained to interview job applicants. This means that you must train yourself to be a top notch interviewee, without having the benefit of being asked the right questions. You have two goals during the interview: finding out if the job is what you want to do, and finding out if you and your prospective boss share the same philosophy. Typically an Agency supervisor will tell you what is being done in the office and a general idea of what your job will be. You will have to ask specific questions about the actual work. In some cases you will want to spend some time with the incumbent or another worker to see what is actually being done. This is the easy part.

If you want to be happy in your new job you also have to reveal a lot of yourself to your prospective supervisor. Tell him or her your worst faults--if he or she can't live with them, neither of you will be happy when those faults come out on the job. You're better off knowing that up front. Also, discuss what you believe to be your virtues and your methods of operation. If you need a lot of independence on the job, say so; you'll chafe under a controlling supervisor. If you need regular feedback on your performance, say so; you'll get ulcers waiting for the strong silent type. Watch and listen carefully to the supervisor during this discussion. Body language and verbal responses to your revelations will tell you more about that manager's style of management than you could ever learn by asking, "What's your management philosophy?"

Be truthful about your intentions during an interview. If you plan to stay in the new job for only two or three years, make that plain. You can contribute a lot during that time, and anyway, there is no stigma to moving; the seniors do so about every two years. If, at the end of your interview, you know that you aren't interested in that job, have the courtesy to tell the interviewer clearly that you are not interested. You might even suggest the name of someone you know who might be a good candidate for the job. If you are considering several other jobs you should tell the interviewer this fact. Play it straight; this same manager may call you years later with a job you do want! □

The following is classified ~~CONFIDENTIAL~~ in its entirety.

ODE

TO THE CA INTERN PROGRAM (u)

P.L. 86-36

[redacted] *B53*

Intern Grads both brave and tough
How we learned that cryptic stuff!

Was that program quite a chore
And that paper quite a bore?

Did we importune our buddies
As we practiced Folklore studies?

Did we grow more fatalistic
As we mastered each statistic?

If we shunned some probability
Did we suffer culpability?

In the washroom did we primp
Rather than practice IMP?

Would we games and puzzles play
Instead of work upon a CRAY?

Or struggle with a CDC
Or, worse yet, some weird SPD?

To choose UNIX or PCDOS
Were we ever at a loss?

Feezy filzy foozy fumzy
Do our brains feel slightly numbzy?

Are we live or are we dead
After so much traffic read?

Now we're Permanent and Real
What's the bravest thing we feel?

DO YOUR WORK, OH CAFETERIA
AFTER THREE YEARS

WE'VE NO FEAR O' YA!

Reprinted, with permission, from the October 1986 issue of the Cryptanalysis Intern Bulletin

A COMPOSITE CONVERSATION (U) Loosely Based on Experience

P.L. 86-36

[redacted] G72

I said, "Boy, I sure could use some computer support! I've got masses of data in this language to process and I need some efficient way to put the good stuff into English."

He said, "Boy, are you in luck! I've got just the thing for you, an interactive, virtual, untra-fast Gizmo Super-X computer with a superpowered, glitch-free VDT that won't even give you eyestrain. It will do everything for you but tie your shoes!"

I said, "But I don't need my shoes tied, I need help translating. Can your machine do that?"

He said, "Of course! It can interact instantaneously in 87 different scripts, including upside-down Urdu complete with all those funny squiggles and dots, whatever they are, I never claimed to be a linguist myself."

I said, "But I do this language, not Medieval Mongol, and my output is supposed to be all in English. I don't compose in all these other writing systems!"

He said, "No problem, we'll just ignore these other scripts, they only cost a few thousand dollars per machine anyway! Now what else do you need?"

I said, "Well, how about a really sizeable dictionary and the capability to look up a term more quickly than I can by hand?"

He said, "Of course you know that will take all your memory. But we can do it! If you'll just fund the typists, we can probably get the dictionary entered in a couple of years! And the neat part is that you can program the dictionary yourself!"

I said, "Me, program? I'm a translator. I don't have time to learn to do all that."

He said, "Not to worry, it doesn't take all that long, I picked it up in just a few weeks myself. Just think, you'll be able to do all your own programming! Only thing is, the course is full and you can't get in until sometime late next year."

I said, "Why can't you do the programming for me?"

He said, "Who, me? I'm too busy for that! I already spend nearly full time as it is working the bugs out of the programs other people write, I don't need another job. You know these systems anyway, they're all overloaded."

I said, "Overloaded already? Then how can I add a program with dictionary, look-up capability, word processing, and all the rest?"

He said, "Well, you really can't for now. But just as soon as we get the Gizmo Super-X, you can do everything since it will stand alone."

I said, "You mean it won't have to talk to all these other systems? But what if I need to do just that?"

He said, "Well, it won't unless we develop a special package, but I'm sure that's already well in hand. Not to worry!"

I said, "So I have to wait for the Gizmo Super-X plus my programming class plus whatever interface package eventually gets developed, all before I can start work? With the budget situation the way it is these days? What do I do in the meantime?"

He said, "Well, if you only knew how to program, you could use your present system for, oh, just lots of things; of course, it's overloaded, so don't try to add too much, maybe just a few working aids or so. And by the way, the word-processing program on that system takes too much system space so we're going to take that out."

I said, "Thanks a lot!"

He said, "Have another pencil."

%

This review is classified ~~CONFIDENTIAL CCO~~ in its entirety.

GCHQ: The Secret Wireless War 1900-1986
By Nigel West. 294 pp. Weidenfeld and Nicholson, London, 1986. [L12.95].

Reviewed by: Vera Filby, E41

This book on NSA's senior partner is a well-organized, well-researched history of British SIGINT beginning with its origins in telegraphy and wireless and carrying through in straightforward chronological order to events current at time of publication in 1986. It is no exposé or Bamford-style effusion, though the author has a reputation for such writing, but a balanced account of what happened, how it happened, and what it means, with abundant detail on organizational developments, complexities, and interrelationships, on codes, ciphers, and cryptomachines, on cryptologic places and events all over the world, and on people. Readers can enjoy the opportunity of learning more about some of the extraordinary people who over the years have made cryptology and SIGINT what they are.

This is also a book for entertainment, as any SIGINT history can be expected to be, since SIGINT in all its intricacy is endlessly interesting and a continuing source of great stories -- stories of achievement, of loss and failure, of discovery, stories of rivalry, international intrigue, war, and betrayal. What a goldmine historians have found to dig in since the ULTRA revelations in 1974! Some, like Nigel West, seem to have developed an understanding and appreciation of SIGINT's special nature. West is a military historian, and this is his seventh book on intelligence matters. Except for some private records of the Radio Security Service, his listed sources are public records and published works.

Until the beginning of the first World War, British authorities preferred to trust the security of their cable links throughout the Empire and were wary of wireless because of its vulnerability to intercept and its potential for spying. When war started, radio amateurs were banned, but eventually they were called upon to help. Future cryptologic organization was foreshadowed in a recommendation to make a list of those who would be willing to be trained in encryption, decryption, censorship, and interception. What was to become SIGINT started when wireless experimenters in the field in France came across German telephone conversations. That was the first surprise. The next was the clear evidence in those conversations that the Germans were intercepting the communications of senior Allied officers. War Office intelligence could hardly miss the significance of this, and soon the first military SIGINT unit was founded. Thereafter and throughout the war, SIGINT became an increasingly indispensable asset for the military forces.

The cryptologic history of the Great War is well documented and its outstanding events - most notably the still controverial battle of

Jutland and the celebrated Zimmermann telegram -- often recounted. West retells this history as an integral part of his total picture.

In an effort to reduce extensive service duplication a new body with the innocuous name Government Code and Cypher School was established on 1 November 1919. With wartime targets gone, GC&CS redirected its efforts to Soviet traffic, which was supplied by Army signals elements, and to Japanese, copied by Admiralty stations. In addition, civil and governmental communications provided a rich supply of Soviet diplomatic traffic, much of which was readable and highly valued for its abundant evidence of Comintern programs of subversion.

In 1920, top British Government officials chose to release decrypts of Soviet telegrams with all surrounding details to expose Soviet undercover activities. No reaction was apparent in Soviet traffic, but then the Government did it again. By the end of 1920 the Soviets were using couriers, and the traffic had disappeared. When it later resumed it was quickly broken and was read until May 1923, when once again the Government blew it, this time to challenge Soviet adherence to a Trade Agreement of 1921 and to support an ultimatum demanding that the Soviets cease financing subversion in Great Britain and the Empire. The price of this political decision was again temporary loss of the traffic. Finally, after yet another deliberate compromise in 1927, the Soviets introduced one time pad. These are the things that break SIGINTers' hearts.

In 1922 the Foreign Office took over administration of GC&CS because it was believed that the central problem for SIGINT would be diplomatic, and it was given jurisdiction over intercept, DF, TA, and CA in order to centralize control over these scattered functions. At that time the staff numbered 91. Led by a few brilliant survivors of Room 40, the organization achieved many successes but remained in a state of underfunded obscurity up to the very edge of war. Only in 1938 was a German section formed. But by the end of 1939, GC&CS had acquired the wartime covername of Government Communications Headquarters, and its staff had grown to 937. The wartime peak, in June 1944, was 6,812.

The Enigma machine enters the story when in 1926 the German Navy began using a version of it. The British Admiralty had bought two machines in 1928, and after years of consideration a Whitehall committee decided to have the Air Force supervise construction of a machine based on it. This became the TypeX, which provided secure telecommunications for Allied SIGINT throughout the war. Experts recognized that Enigma machines, in all their versions, were impenetrable if used correctly. But with thousands of German Enigmas in use, and under all kinds of conditions of stress and crisis, errors did occur, and these compromises did help the cryptanalysts break into systems. The fact that error can make systems vulnerable is well understood, and it is therefore rather surprising that the author makes so much of it. It is his view that this truth is the real ULTRA secret.

istorians seem to have been so intrigued with codes and ciphers and so involved in reevaluating battles, campaigns, and diplomatic maneuverings in the revealed context of intelligence that they have been less concerned with researching the fundamental role of intercept. At the time of his death, Ronald Lewin, author of *ULTRA Goes to War* and *The American MAGIC* , was compiling materials, now deposited in Churchill College, Cambridge, for a study of the British military intercept services, which have been coordinated by the Y Committee since 1928 and are referred to as the Y Service. *The Story of the Y Service* was the subtitle of Aileen Clayton's excellent history (and great adventure tale) of her wartime RAF service, *The Enemy is Listening*, published in 1980. West has now added to this record his account of the Radio Security Service.

True to the tradition started in World War I, wireless amateurs volunteered to help the war effort. Their help was sorely needed because

Foreign Office and Special Service facilities were ineffective or inoperative. The role of these Volunteer Interceptors when they were organized into the Radio Security Service in 1939 was to cover agent communications. By March 1940 they had completed their mission - the target had been eliminated. Meanwhile they had been copying great quantities of enemy signals from the Continent, developing techniques, and building data bases. Of their contribution, West says that "it was largely due to them that the cryptographers at Bletchley Park were able to continue their work."

A history of GCHQ necessarily includes a history of NSA, and West begins his treatment with the closure of the Black Chamber in 1929 and continues it as part of a combined story up to the present. Negotiations between Britain and the United States began in 1940, and the next year a replica of the PURPLE machine, which produced decrypts, designated MAGIC, of Japanese diplomatic messages, was sent to GCHQ headquarters at Bletchley Park (also known as BP, Station X, and to the Navy, HMS Pembroke). PURPLE had by then survived an appalling leak, when American authorities disclosed to the Soviet ambassador information in a MAGIC decrypt concerning Hitler's intention to invade Russia.

But those who, as it turned out, could have profited most from MAGIC did not have access to it. In his brief summation of Pearl Harbor, West notes that the commanders were out of the loop and that the low level tactical traffic that would have warned them was processed, after delay, in Washington, where the strained resources were committed to traffic of presumed higher value.

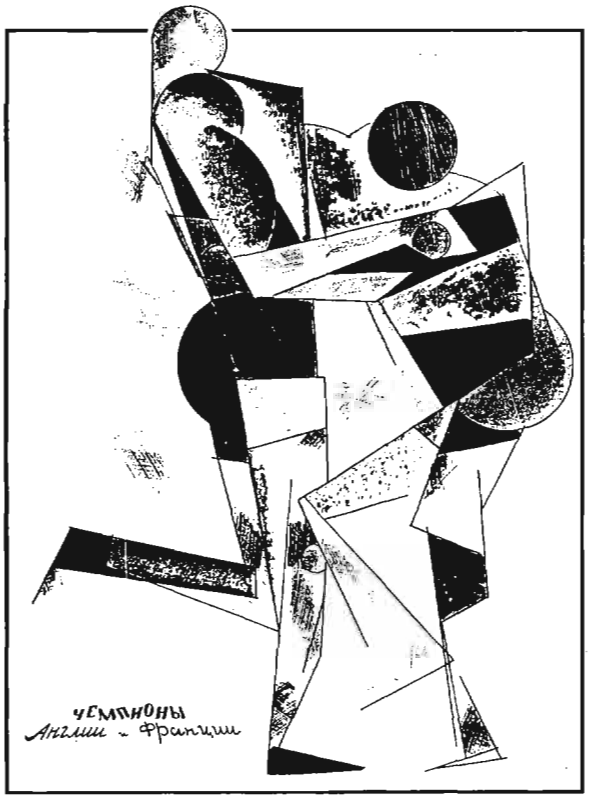
UK and US SIGINT collaboration was formalized in the BRUSA Agreement of 17 May 1943. This and later agreements with Australia and Canada established the basis of the structure that exists today. So productive was the collaboration that by the end of the war the SIGINT effort was flooding intelligence channels with torrents of information.

clever author likes to surprise his readers every now and then, and West does so by switching suddenly from the SIGINT scene at the end of the war to Australia. In 1944 a station there -- of all places -- picked up Soviet traffic in a system codenamed VENONA. This event, West believes, helped set the stage for a peacetime mission in exploitation of Soviet clandestine traffic. This traffic revealed continued Soviet involvement in and support of international subversion -- the story of the 1920s, unchanged. Exploitation of VENONA led eventually to the identification of the spy, atomic scientist Klaus Fuchs, the traitor Donald Maclean, and other spies and traitors in the ramifications that continued for years.

The last two chapters of the book, covering the postwar period, portray a scene of continual disasters, from the shooting down of the EC-130 over Armenia to Prime and the Pelton case. This is not really surprising, since only the things that go horribly wrong get out to become meat and drink for historians and investigative reporters. But such a recitation of losses, leaks, compromises, defections, and multiyear penetrations leaves a SIGINT reader feeling like a farmer who has seen his entire community's long-nurtured crops wiped out by insects and disease. The author manages to wind up, however, on a positive, if cautionary, note: "The secret wireless war will continue for as long as there are communications to be intercepted and signals to be interpreted. Accordingly, GCHQ will remain an invaluable source ... and a tempting target."

This book has been faulted for lack of proper, scholarly footnoting and original research. Be that as it may, for readers who want only a consolidated, readable survey of the publicly available record it will do the job. □

TECHNICAL LITERATURE REPORT



ABSTRACTS ON

SOVIET PACKET NETWORKS (U)

P.L. 86-36

Reported by: [redacted] *P13*

The June 1984 issue of *Inspec Key Abstracts on Communication Technology* contains translated abstracts of papers presented at the 3rd All Union Conference on Computer Networks for Packet Commutation (Вычислительные Сети Коммутации Пакетов, Тезисы Докладов Третьей Всесоюзной Конференции) in Riga, Latvia, in September 1983. The Russian proceedings were published in two volumes with abstracts in each volume. One foreign network, the Spanish IBERPAC, was described in the translated abstracts reported here.

One of the papers notes problems in implementing X.25 that result from the lack of a standard formal description of X.25 (and X.21). In Bratislava an experimental computer network IPK is being developed using the ISO architecture. The SIMULA 67 language was used to investigate the 4th layers of the protocol. A 'problem oriented' network 4 SET is a distributed computer system based on the IZOT 1016 small computers and the SM-4 mini computers. The SM-4's are connected to one another by data transfer channels, and form a network which operates across large distances. A term 'teletreatment of data' is introduced in connection with a description of the experimental packet switching network SET 1.2. The possibility of using optical fiber links for high speed transmission to perform 'distributed data treatment' is investigated in one paper.

Six papers deal with LANs. Foreign LANs such as ETHERNET, IEEE Project 802, ECMA, Sinpads and Hypernet are investigated to determine the control functions and access functions. No specific Soviet LAN is mentioned.

An interesting feature of the conference is the variety of different LAN and packet net schemes presented. There does not appear to be a single national system, and some of the regional systems link into the AKADEMSET net. This shows local variety that seems surprising in the centralized Soviet system.

The Soviet Academy of Sciences uses an AKADEMSET packet switched network for internal and foreign information-computing resources. The Ministry of Communications, and parties with data bases and applied software can also use the AKADEMSET network. Elektronika 100-25 minicomputers are interfaced by hardware adapters to the BESM-6 computers, and the whole structure used as an interface machine for accessing the AKADEMSET network. The SM-4 (TISA-4) has also been proposed as an interface with the packet network AKADEMSET. X.25 packet transmission protocol is used to connect the ES-7920 computers to the packet switching center in an open network.

There is apparently more than one packet net development, and several different services. A subsystem EKRAN of the DNEPR computer network is used for electronic mail. A network of the TsSu SSR provides user services which include: transfer of single- and multiple-address information; virtual communications between two points; data collection by computer

from user terminals; dialog communications between networks users; and operator-user communications. The MSSR Academy of Sciences has developed a distributed computer network for quick access by a large number of users to an automated data base of scientific information. A multifunctional terminal system of a scientific center uses a central SM-4 minicomputers and peripheral Electronika-60 microcomputers, connected through the recommended X.25 protocol. This provides software exchange, collective use of external system hardware and simultaneous remote interaction among several users.based on variable packet lengths less than 1K, and data transfer speeds between 50 kbytes/s and 1 Mbyte/s.

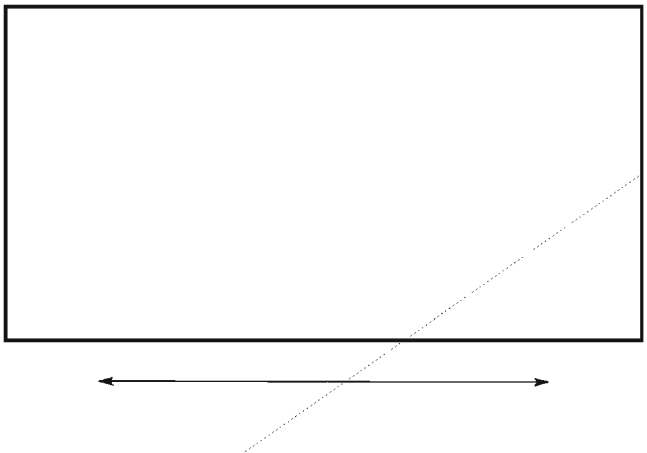
A Terminal VTsKP network for regional control of internal affairs combined different computers into a single distributed terminal network, using hardware developed along the CAMAC standard. A regional computer subsystem 'Ural' is intended to give users a wide range of services, including remote access to the subsystem informational-computational abilities, as well as access to the AKADEMSET network. The DNEPR network has a communication network that will accommodate 255 ports, receive or send messages up to 27 Kbytes, and remotely open or close ports.

A synchronous communication controller was developed to do bit-by-bit signal treatment using HDLC (high-level data link control), SDLC (Synchronous Data Link Control), and "K.25/2" (probably a typo for X.25/2) type protocols . The interface is intended for a microcomputer and connects with the main bus from one side and with either a synchronous or an asynchronous modem. The use of a subsidiary processor to free a main computer from queues of data will prevent inefficient data treatment even though it makes the net more complicated. One paper proposes the use of a TISA-4 computer to provide interface for a complex of SM-4 and BESM-6 computers with the AKADEMSET network via the network access method in TISA-4. Another proposal would use specialized hardware to perform the lower levels of the packet switching protocols to free the computers for more problem solving. A "cylindrical magnetic domain memory" (perhaps some kind of drum or disk) system of 100 Kbytes is proposed to give a reliable storage for storage of systems software and initial loading of separate microprocessors in the network.

X-25 is the standard packet mode transmission in more than 50 packet switched data networks that are operating in other countries. It is a CCITT recommendation for a packet protocol which makes a universal interface feasible between data terminal equipment and public packet switched networks. It is defined on three levels, viz: physical, link and packet level. The digital communications are defined by CCITT Recommendations X.20 and X.21 for stop-start and synchronous communications, and most existing packet nets support data rates of 2.4, 4.8 and 9.6 kb/s. Some also offer 48 or 56 kbps. The Soviets are currently using modems on some circuits which meet CCITT 4.8 kbps specifications. One of the Riga papers specifies a LAN.

Analysis

The US began its development of packet networks about eighteen years ago with ARPANET, which had heavy university and laboratory participation. Since then a number of packet nets have developed, many with scientific and resource-sharing aims. The Soviet AKADEMSET appears to be a development along similar lines. The technical features, as far as can be determined from the abstracts, are centered around micro and mini computers and medium-speed data modems. The work is probably about ten years behind US applications.



Letter

P.L. 86-36

To the Editor:

(U) I chuckled to myself the other day as I read [redacted] introspections into the misty world of collection management. I think we all go through this period of doubt and reassessment occasionally - I know I have. Whether it is brought on by the myriad of reorganizations we have experienced; by endless criticism; or by mid-life crises, it is probably healthy to step back periodically to recount and reassure ourselves. (i.e., Now that you are a professional collection manager, what are you expected to do for a living?)

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

~~SECRET~~

[redacted]

(U) Just where does the real collection manager fit into this process? Right smack in the middle with both feet! Using his experience he must teach, cajole, reprimand, negotiate, and concede all in the course of a day. He is totally dependent upon analysts and collectors alike and must be guided by his NSRL. His responsibility is endless; his authority is elusive. The collection manager is the catalyst that makes it all work -- whoever he is.

(U) If [redacted] still has doubts about the necessity for collection managers, I suggest that the Collection Association consider instituting counseling sessions to coax [redacted] and any other temporarily wayward collection managers back into the mainstream of NSA thinking. Ours is a noble profession, no matter who does it.

[redacted] *P53*

~~(S CCO)~~

OPPORTUNITY

- Are you a traffic analyst who despairs of finding a good TA job?
- Are you a risk-taker who likes independence and responsibility?
- Are you still searching for excellence?

If your answers are yes to the above, come talk to us. Regardless of grade, we may have just the job for you. [redacted] target is getting a lot of attention and will be receiving more.

We're searching for a few excellent men and women. If you think you are one of them, call [redacted] G221, on 963-3895s.

~~(S CCO)~~

BULLETIN BOARD

FOR CRAY USERS

~~(FOUO)~~ Cray Research, Inc., has a quarterly publication called *CRAY Channels* for users of its computer systems. If you are interested in obtaining a copy contact [redacted] CRYSCOM exec, A53/P13, 963-4196.

ATTENTION: LINGUISTS WITH IBM-PCs OR COMPATIBLES

(U) [redacted] is an on-line dictionary-building and look-up tool designed for the IBM pc or compatible running DOS 2.0 or above with two disc drives (floppy, fixed and/or cartridge.). It is memory-resident and requires 140K of RAM, in addition to whatever your word processor needs. According to the specifications, it works with Word Perfect, MultiMate, VoksWriter Delux, Word Wand, Palantir, WorldWriter, and other word processors. It also is said to work with pfs:Write and WordStar, but the latter two do not accept accented characters. Anyone interested in experimenting with this as yet untested software (it came as a free sample in the mail) is invited to call or write [redacted] P16, 963-1103s.

INSTITUTE ON MACHINE TRANSLATION

(U) Georgetown University, Division of Interpretation and Translation, will offer an Institute on Machine Translation from August 10 - 14, 1987. Persons who had participated in the 1985 Institute may register just for the sessions on new material, which will be given on 13 and 14 August. Fees are $200 for the five-day Institute, and $120 for the two-day sessions.

(U) Topics to be presented include basic issues of MT, recent developments in the field, and future trends.

(U) For further information and applications contact [redacted] P16, 963-1103.

ATTENTION ROCKET WATCHERS

~~(FOUO)~~ The History Division, in cooperation with W1, is undertaking a historical study of DEFSMAC and its predecessor organizations, SMAC and the A4 Watch. If you have records coyering those orgnizations, or have personal knowledge of significant organizational or substantive events, please call [redacted] or Henry Schorreck at 972-2355. You may also write them at T542, SAB 2 Door 3.

FOR SPANISH LINGUISTS

~~(FOUO)~~ Still a favorite and available is the 1981 reprint of *SPANISH VOCABULARY, A Translator's Aid*, P1 Language Publications No.15 (S-220,300) 1979, compiled by [redacted] Copies can be obtained from [redacted] P16, HQ 8A187. Mail orders only are accepted.

CISI

SPRING CONFERENCE

Theme: INFORMATION SECURITY

18-22 MAY 1987

‡

GENERAL SESSIONS

Friedman Auditorium

Daily, 0900-1130 and 1300-1500

‡

CONCURRENT TECHNICAL SESSIONS

FANX II

National Cryptologic Course Center

Tuesday, Wednesday, Thursday

(Complete program with topics, speakers, and schedules will be published soon)

‡

For further information contact one of the Conference Co-Chairmen, [redacted] X2, 987-7446, or [redacted] P34, 963-6119

THE STORY OF A PRIVATE GERMAN CIPHER OF WW I (u)

(Aug-Sep 1986)

[redacted] A204

The postcards were found in a flea market in Stuttgart in 1979 or 1980 by Tom Brousseau while we were both assigned to Europe. Tom showed me the postcards, and though I found the cipher not difficult, the German script and language presented a problem, so we set them aside. In 1983 Tom lent me the cards for another attempt, and while I was at it [redacted] a co-worker in A2 and a good German linguist, strolled by, and soon read them. The only problem was interpreting a phrase in Martin's card to Anna, which we believe reads, "Today I finished preparing the flower vases."

Then when Frank was nominated to study at USARI in Garmisch, we thought it would be fun if he would go Stammbach, which we learned is about 20 miles north of Beyreuth, and check the local cemetery and the records at the town hall. But we really had no expectation of finding any trace of Anna or Martin, as 70 years had passed since the postcards were mailed.

When Frank got to Stammbach in 1986, he learned that Martin was born in 1884, and that Anna was born in 1884 and died in 1949. They had no children.

How Frank found the information and what happened as a result is a story in itself. To summarize briefly, he simply walked along the street where his pension was located, saw a grocery store owned by one Karl Wirth, and told a salesclerk that he was seeking information about Martin and Anna Wirth. One thing led to another, and he met a host of Martin and Anna's relatives, among them Martin's niece Anna, who told him that Martin had died in France in 1915. (The postcard shows him alive in January 1916. It is likely that Martin was killed during the battle of Verdun, which began with a German offensive on 21 February 1916, with heavy casualties on both sides.)

Frank had such a good time in Stammbach that he spend the next five days there, not speaking a word of English.

The niece Anna, who now lives at the address of her Aunt Anna on the postcard, was perplexed about the postcards. How did they end up in a flea market in Stuttgart, she wondered. As do we.

But there's something else that puzzles us more. How was it possible that correspondence in cipher between a soldier and a civilian was permitted in time of war? Granted, it was a simple cipher, transparent to a professional. But what about the enigmatic message? The German linguists who looked over the decrypted text agree that the that cryptic passage is best translated, "Today I finished preparing the flower vases." But it seems an unlikely undertaking for a soldier, albeit a horn player, especially in January. Could it be a private message with the meaning, "I'm going to the front"? Perhaps some reader has the answer.

Among the difficulties we faced in translating the text–the cipher posed no problem–is that the postcards were written in pencil, and that the writing, in hard-to-read old-fashioned German script, is smudged. Furthermore, the spelling is non-standard; it is thought to reflect a local dialect. So other readings for the puzzling phrase cannot be ruled out.

THE CIPHER

1 2 3 4 5 6 7 8 9

A E I O U L M N R

CARD FROM ANNA

LIEBER MARTIN!
BIN GESTERN GANZ GUT
NACH HAUSEGE KOMMEN
VON NEUEMARKT BIS HEIM
2.E KLASSE GEFAHREN BIN
HEUTE GANZ AUFGEREGT
LASSE RECHT BALD ETWAS
VON DIR HÖREN ODER
KOMME SELBST NOCH EINMAL
HEIM MIT HERZLICHEN
GRÜSSEN DEINE TREUE ANNA
HABE DEINE UHR SELBST MIT
ZUM UHRMACHER GEBRACHT

Dear Martin
I arrived home well yesterday.
I travelled second class from
Neuemarkt. Today I am
very excited. Let me
hear from you soon or
come home again. With
heartfelt greetings
Your true Anna
I brought your watch
to the watchmaker myself.

CARD FROM MARTIN

LIEBE ANNA
DEIN WERTES KARTCHEN
MIT FREUDE ERHALTEN
BEI UNS IST DAS WETTER
SEHR SCHON DIE BLU
MENVASEN HABE ICH HEUTE
FERTIG GEMACHT ES GRÜSST
DICH BESTENS DEIN LIEBER
MANN MARTIN

I was please to receive your dear little card.
We are having very beautiful weather.
Today I finished preparing the flower vases.
Best regards from your
loving husband Martin.

Solution to:

WHEEL OF FORTUNE

(Oct-Nov 1986)

1. WILLIAM FRIEDMAN
2. ARLINGTON HALL
3. CIPHER CLERK
4. DOUBLE TRANSPOSITION
5. BOOKBREAKERS FORUM
6. BURN BAG
7. CALLSIGN ROTA
8. ROTA SPAIN
9. DEPTH READING
10. CHELTENHAM
11. ONE-TIME PAD
12. BLETCHLEY PARK
13. SPREAD SPECTRUM
14. AIRPORT SQUARE
15. PLAYFAIR SQUARE
16. NORMAL DISTRIBUTION
17. FOR OFFICIAL USE ONLY
18. COMMUNICATIONS SECURITY
19. ZIMMERMAN TELEGRAM
20. HAGELIN MACHINE

Because of Technical Difficulties
We are Experiencing Delays
in Producing CRYPTOLOG

NSA-CROSTIC (+) No. 63

by [redacted] P12

Of all the puzzles that appear in CRYPTOLOG, the NSA-Crostic is by far the favorite. We're happy that in this issue we can satisfy the requests of many readers. This particular NSA-Crostic has an added wrinkle. Is it a clue or a bonus? That depends on when you hit upon it. It's a clue if you find it early enough, or a bonus if it becomes evident after the fact.

A. Insouciant
B. Normal personnel loss
C. Hybrid bramble
D. Mu's neighbor
E. Reddish bird dog (2 words)
F. A family ruler
G. Diligent
H. Innate
I. Syncopated?
J. Fortify
K. Essay
L. Supply fully
M. Patron
N. Crowning achievement
O. Casual
P. Plane figure; not a Greek conflict
Q. On edge
R. Apartment
S. —— del Vaticano
T. Seminary subject
U. Victim of Paris
V. Water nymphs; not dryads
W. A cryptanalytic phenomenon, such as TT; medieval garb
X. Amateurish

37	22	115	195	3	97	26	75			
112	61	48	66	85	77	21	106	187		
148	134	14	141	76	62	2	179	38	57	
185	120	74	153	36	13					
12	173	4	60	130	168	73	182	162	109	110
127	149	189	72	100	90	161	20	176		
180	47	183	131	11	88	16	158	147		
108	103	30	92	1	71	105	42	124	166	
128	64	50	52	29	137	70				
84	56	193	160	5	79	89	163	69	43	
118	138	143	63	99	121	94				
104	67	40	191	177	33	6	17	82		
86	133	49	25	126	184	68				
159	65	28	80	170	18	190	93	114		
169	117	181	171	44	194	102				
119	186	15	51	91	172	146				
58	125	150	7	35	136	154				
151	129	167	31	155	19	98	10	135	39	
34	53	174	175	78						
107	156	192	123	54	9	188	46			
24	178	122	83	95	165	32	142			
101	145	8	157	113	96	140				
152	116	59	87	45	139	81				
55	23	164	27	132	111	144	41			

1 H	2 C	3 A	4 E	5 J	6 L	7 Q	8 V	9 T	10 R		11 G	12 E
13 D	14 C	15 P	16 G	17 L	18 N	19 R	20 F	21 B	22 A	23 X		24 U
25 M		26 A	27 X	28 N	29 I	30 H	31 R	32 U	33 L	34 S	35 Q	36 D
	37 A	38 C	39 R	40 L	41 X	42 H	43 J	44 O	45 W	46 T	47 G	48 B
	49 M	50 I		51 P	52 I	53 S	54 T	55 X	56 J	57 C		58 Q
59 W	60 E	61 B		62 C	63 K	64 I	65 N	66 B	67 L		68 M	69 J
70 I	71 H	72 F	73 E	74 O	75 A	76 C	77 B		78 S	79 J	80 N	
81 W	82 L	83 U	84 J		85 B	86 M		87 W	88 G	89 J		90 F
	91 P	92 H	93 N	94 K	95 U	96 V		97 A	98 R	99 K	100 F	101 V
102 O	103 H	104 L		105 H	106 B		107 T	108 H	109 E		110 E	111 X
112 B	113 V	114 N	115 A		116 W	117 O		118 K	119 P		120 D	121 K
122 U	123 T	124 H	125 Q	126 M	127 F		128 I	129 R		130 E	131 G	132 X
133 M	134 C	135 R	136 Q	137 I	138 K	139 W	140 V		141 C	142 U		143 K
144 X	145 V	146 P	147 G	148 C	149 F	150 Q	151 R	152 W		153 D	154 Q	
155 R	156 T	157 V	158 G	159 N	160 J	161 F		162 E	163 J	164 X		165 U
166 H	167 R		168 E	169 O		170 N	171 O	172 P	173 E	174 S		175 S
176 F	177 L		178 U	179 C	180 G	181 O	182 E		183 G	184 M		185 D
186 P	187 B	188 T		189 F	190 N		191 L	192 T	193 J	194 O	195 A	

Puzzle fans are invited to try their hand at compiling an NSA-Crostic, with or without additional features. For helpful hints and guidelines consult the Puzzle Editor.

~~SECRET~~