

~~TOP SECRET~~

NATIONAL SECURITY AGENCY  
FORT GEORGE G. MEADE, MARYLAND

# CRYPTOLOG

NOVEMBER 1977



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

P.L. 86-36

OBJECTIVE SATISFACTION SCORE: COLLECTION.	[REDACTED].....1
DIRECTOR'S MEMORANDUM: [REDACTED]	[REDACTED].....2
CURE FOR TIME-IN-GRADE SYNDROME.....	Vice Admiral B.R. Inman.....7
A LITTLE T.A. PROBLEM.....	[REDACTED].....9
BACKING INTO LANGUAGE ACQUISITION.....	[REDACTED].....10
NSA-CROSTIC No. 10.....	[REDACTED].....11
HOW MANY AFRICAN COUNTRIES CAN YOU SPOT?..	A.J.S.....14
LANGUAGE PROCESSING FORUM.....	[REDACTED].....16
C.A.A. NEWS.....	[REDACTED].....17
WHAT EVER DOES "HOWEVER" MEAN?.....	[REDACTED].....18
LETTERS TO THE EDITOR.....	[REDACTED].....19
	[REDACTED].....21

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)  
Exempt from GDS, EO 11652, Category 2  
Declassify Upon Notification by the Originator~~

# CRYPTOLOG

Published Monthly by P1, Techniques and Standards,  
for the Personnel of Operations

VOL. IV, NO. 11

NOVEMBER 1977

PUBLISHER

WILLIAM LUTWINIAK

### BOARD OF EDITORS

Editor in Chief.....Arthur J. Salemm (5236s)

Collection..... [redacted] (8955s)

Cryptanalysis..... [redacted] (4902s)

Language..... [redacted] (5236s)

Machine Support..... [redacted] (5303s)

Mathematics.....Reed Dawson (3957s)

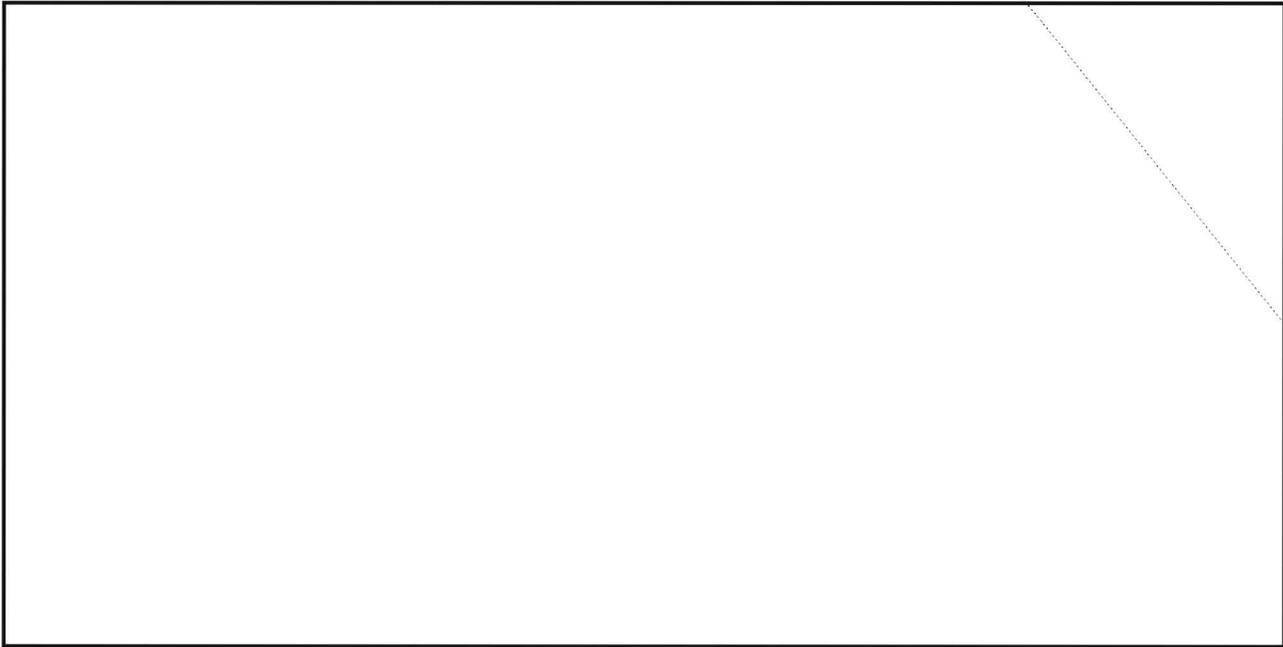
Special Research.....Vera Filby (7119s)

Traffic Analysis..... [redacted] (4477s)

Production Manager.....Harry Goff (4998s)

P.L. 86-36

For individual subscriptions  
send  
name and organizational designator  
to: CRYPTOLOG, P1

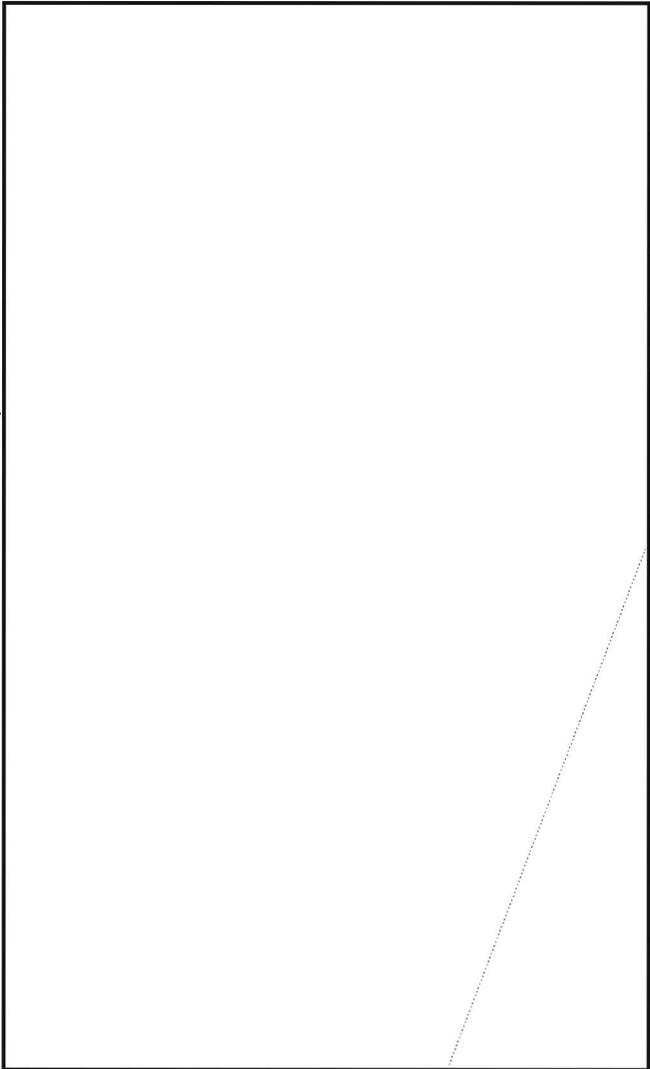
~~TOP SECRET UMBRA~~

One of the major efforts of the intelligence community has been the monitoring of the development and testing of Soviet missiles. The main sources of data for this purpose are provided by the reception and exploitation of instrumentation test signals that the Soviets transmit to assist their engineers in testing and evaluating these weapon systems. The instrumentation signals, along with beacons and space vehicle command signals, are commonly referred to as telemetry.

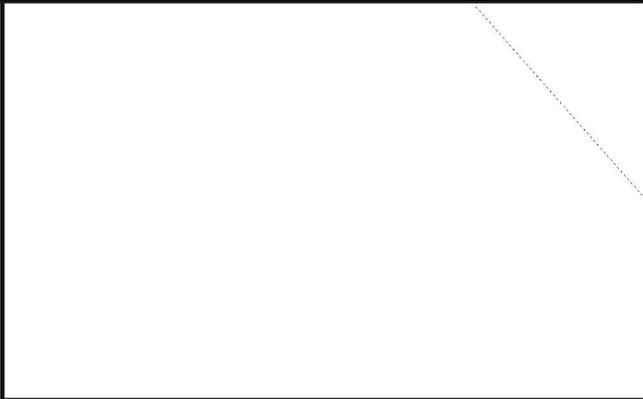
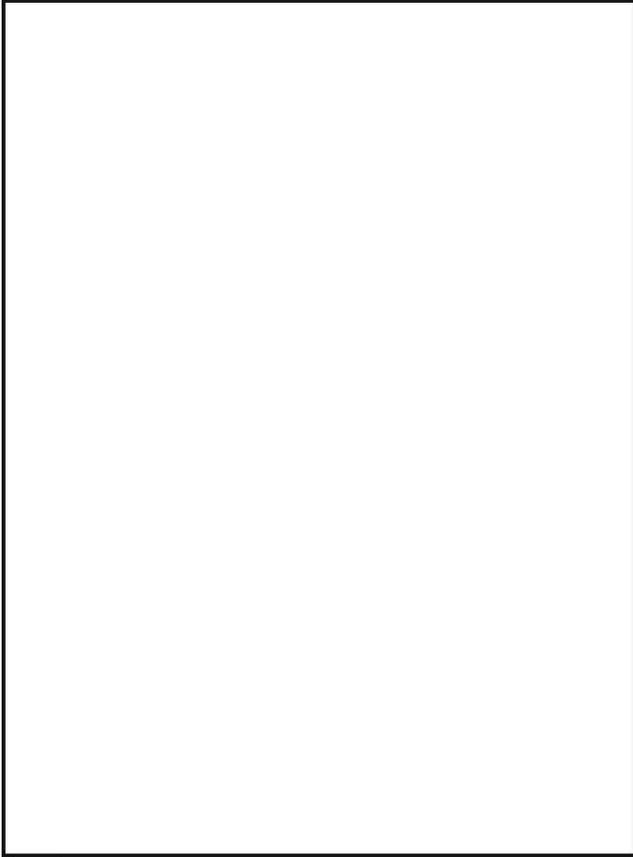
The following paragraphs provide information about a new direction in telemetry -- the making of *external* measurements of missile transmissions -- and give some insight into the application of this development in W1, the Office of Space and Missiles.

Background

As a result of the decreasing availability of exploitable telemetry internals (i.e. the data transmitted to monitor critical missile parameters like fluid flow and acceleration) -- either because of encryption of that data or because of low received-signal strength -- the Scientific and Technical Intelligence Community (e. g. MIA, FTD) has been forced to explore the area of externals data. It is of extreme significance that, from the external characteristics of the signal, the community can now recover data on weapon systems that would otherwise not be available.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



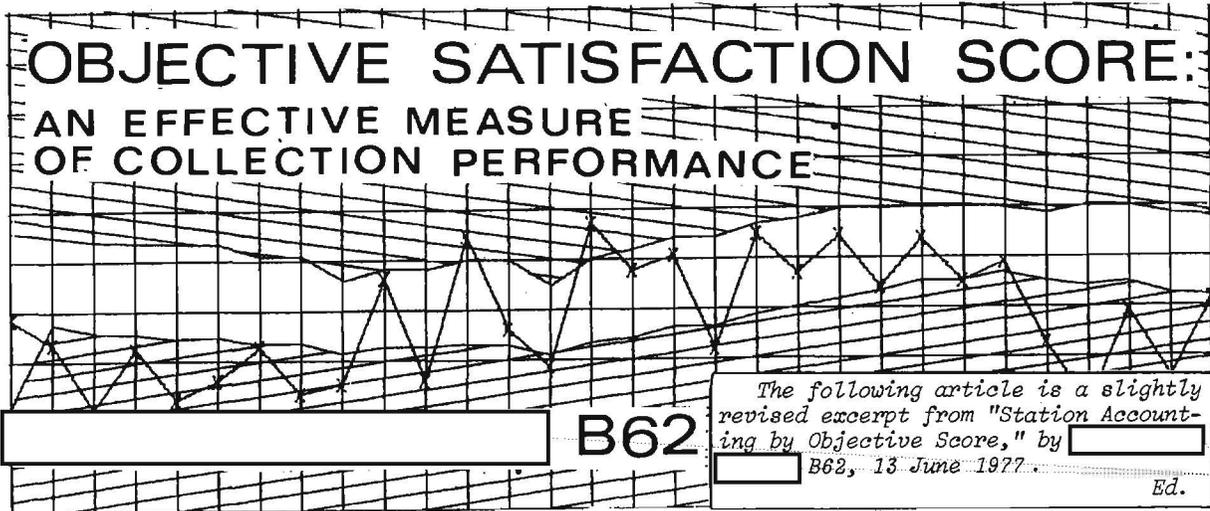
Conclusion

The extraction and uses of externals data require the continued interaction of experienced signal analysts with experienced missile system analysts so that each extracted characteristic can be identified as a parameter of interest or discarded as a byproduct of interference, collection, recording, or processing.

In general, externals telemetry data alone does not permit determination of the missile capabilities. The externals data must be used in conjunction with other data types (e. g., internals, models, simulation programs) to obtain the highest confidence estimates of Soviet missile capabilities.

~~(TSC)~~

~~(SC)~~

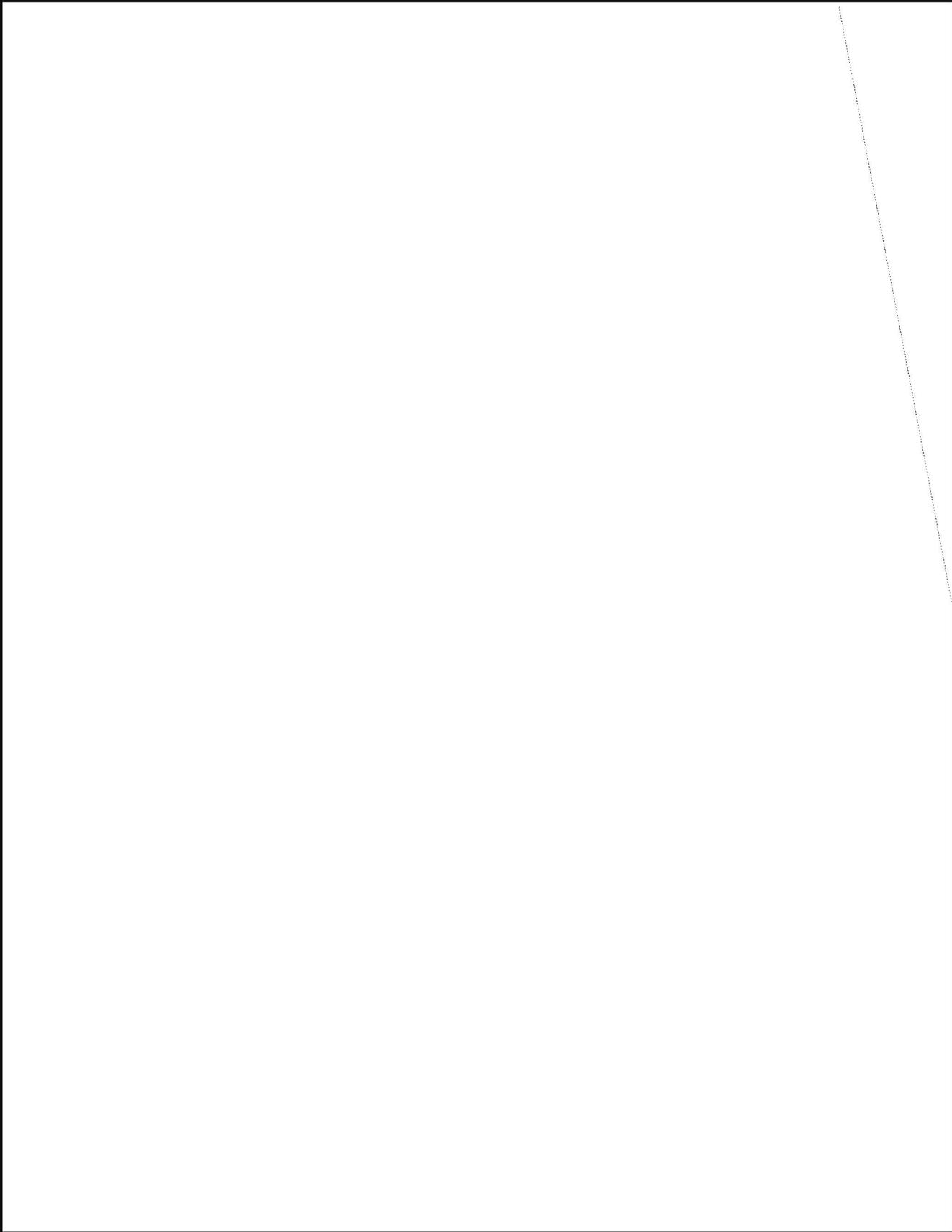


P.L. 86-36

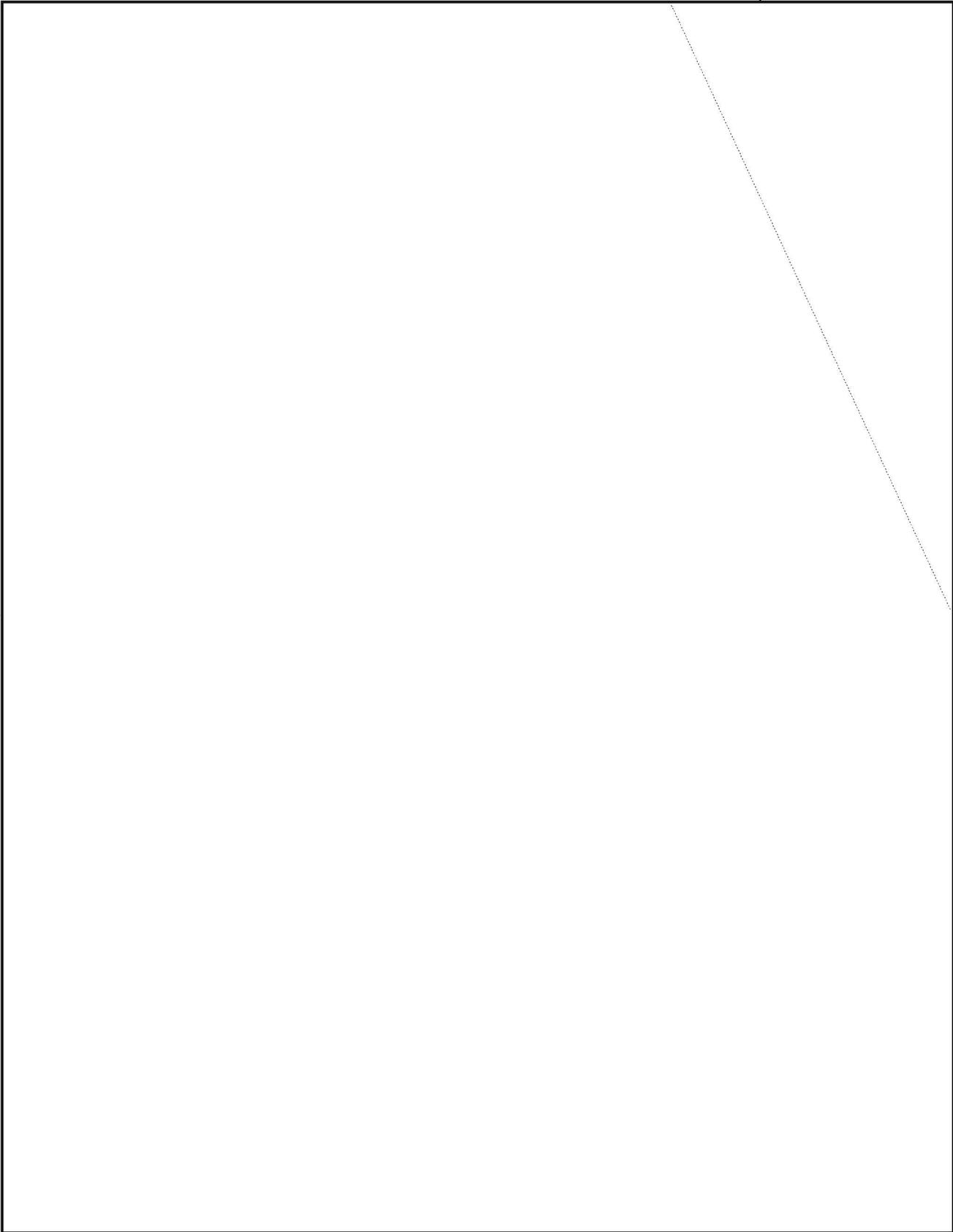


~~TOP SECRET UMBRA~~

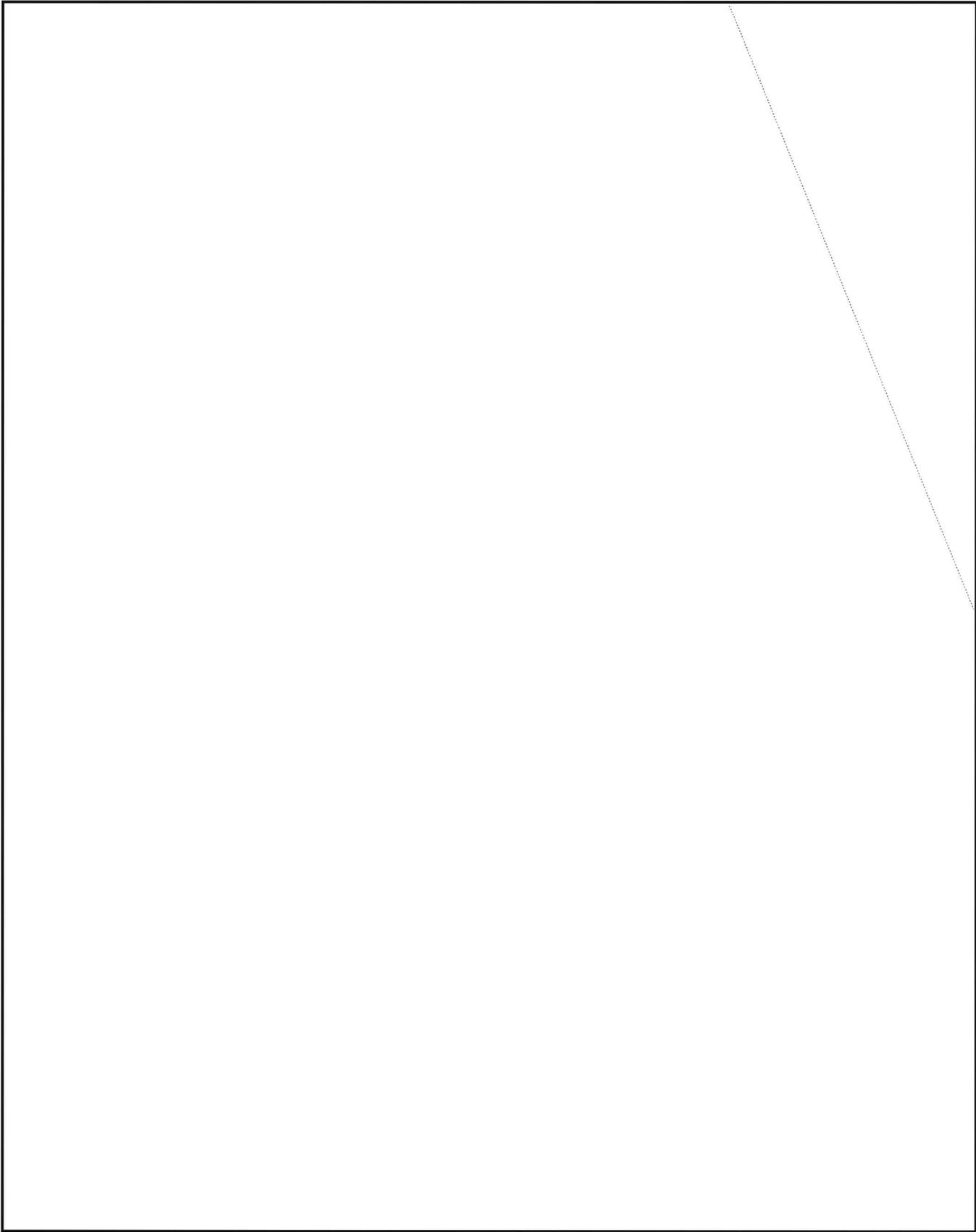
~~SECRET SPOKE~~



~~SECRET SPOKE~~



~~SECRET SPOKE~~



~~SECRET SPOKE~~



~~CONFIDENTIAL~~

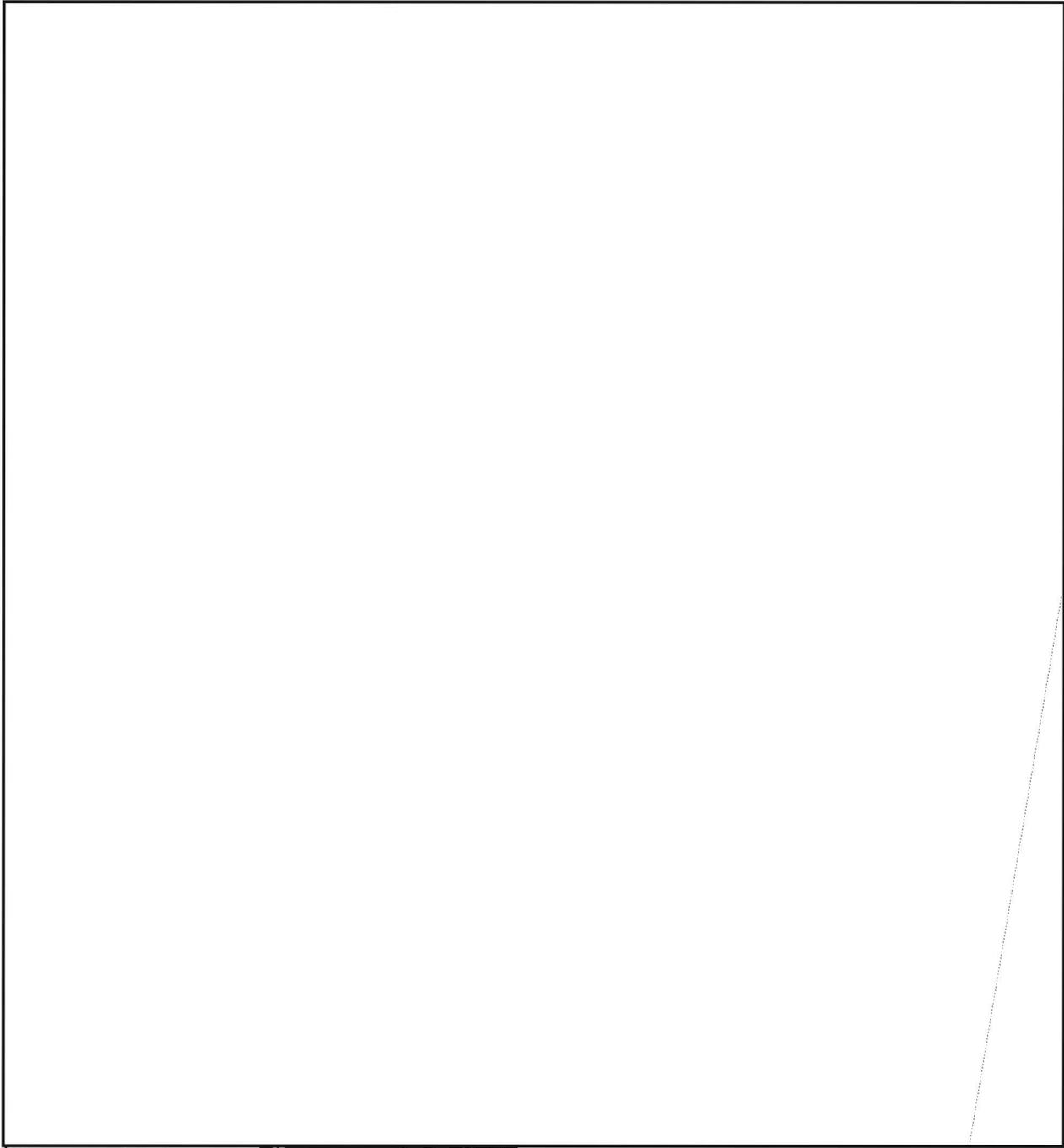
EO 1.4.(c)  
P.L. 86-36

# DIRECTOR'S MEMORANDUM: [REDACTED] GUIDANCE"

Recently I came across a copy of the Director's 4 August 1977 Memorandum and was greatly impressed by its clarity and succinctness. Since a fairly large percentage of the Agency's population is not as well informed as might be desired concerning the objective of [REDACTED] and the constraints and considerations to be applied to that program, I requested the Direc-

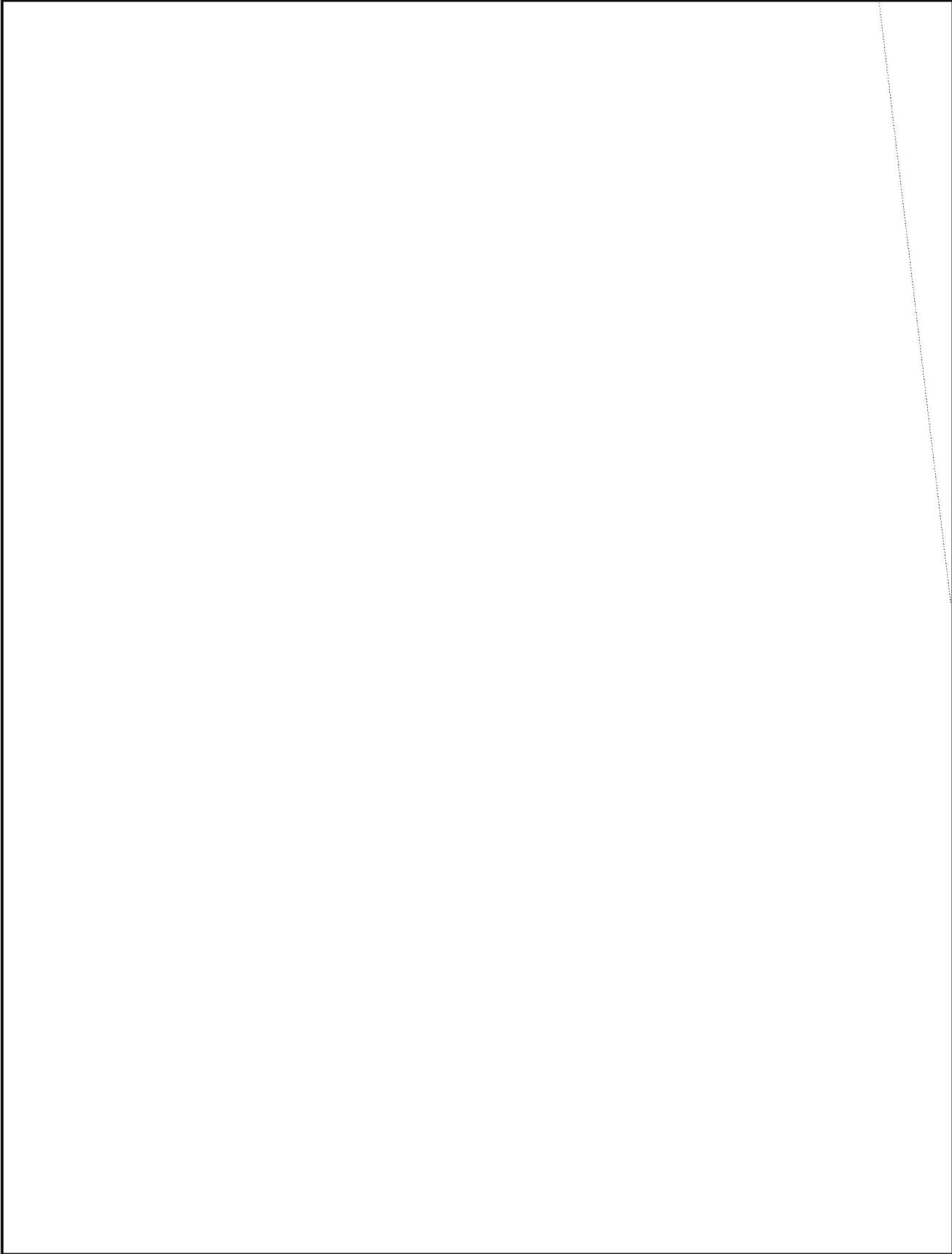
tor's permission to reproduce the Memorandum in entirety in CRYPTOLOG. In that way, we could inform our readers of what the program will entail. The Director has graciously granted that permission and we are pleased to reproduce the Memorandum in this issue. [REDACTED]

*Collection Editor*

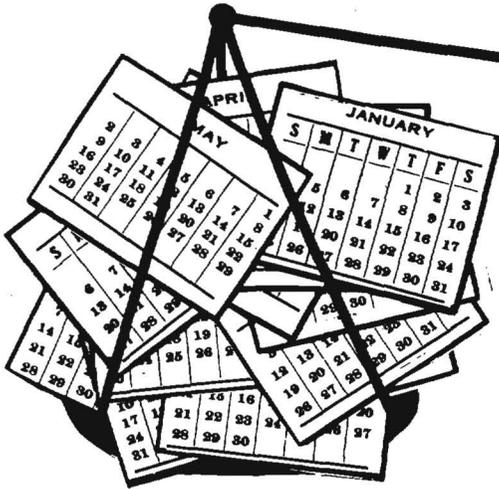


~~CONFIDENTIAL~~

~~CONFIDENTIAL~~



~~CONFIDENTIAL~~



## A PROPOSED CURE FOR THE TIME-IN-GRADE SYNDROME



[REDACTED]

**B311**

Following a recent promotion ceremony, several employees were overheard discussing the merits of the people who had been promoted. Generally their comments concerned the time in grade of those recently promoted, and how that time in grade compared to that of known contemporaries. There was only an occasional reference to professionalization. But there was absolutely no comment about performance. That conversation was typical of those heard daily in almost any element within the Agency. Invariably, whenever promotions are discussed, the first question concerns how much time in grade the person had. Rarely does performance enter into these discussions. The failure of even employees themselves to consider performance or capability is a widespread problem which I have labeled the "time-in-grade syndrome."

The time-in-grade syndrome permeates NSA, as well as other governmental agencies, and is fostered by promotion and pay policies, job assignment criteria, and the employees within the system. It grew from the once-popular belief, still expounded by American labor unions, that management should reward its employees for long and faithful service. This belief was substantiated by using the argument that experience is necessarily the best teacher and thus was a prerequisite for adequate job performance. In other words, performance was only an outgrowth of experience.

The use of experience as a criterion developed from the primitive societies where invariably the oldest men occupied the highest positions. Our society, although not rigidly following this practice, is partially an "age-graded society"

where age, position, and prestige are positively correlated. These practices, ingrained since birth, tend to proliferate and strengthen the time-in-grade syndrome.

Fear of subjective criteria for performance evaluation has also fostered the time-in-grade syndrome since time in grade is a relatively easy criterion to establish and denies charges of favoritism or discrimination. In fact, many still believe that seniority is the only really valid promotion consideration. These people believe that granting promotions to those with extended time in grade is a way of rewarding the employee for loyalty and devotion. No one would deny that loyal service deserves some reward, but no supervisor can get effective results with people if there are limitations in the opportunities to make the best use of subordinates' capabilities.

Advocates of the time-in-grade criteria hold that ability increases with service, especially in the lower-level jobs on the promotional ladder. No doubt this is true in the beginning formative years of an employee's career, but, beyond a certain level, continued length of service at the same level actually *reduces* an employee's ability by producing what is referred to as "a trained incapacity"\*.

\* "The employee becomes so inbred with the problems and procedures of his present job that he is unable to adjust to new circumstances and situations. The expert becomes too expert." See: James J. Healy, "The Ability Factor in Labor Relations," *Arbitration Journal*, Vol. X, No. 1 (1955), pp. 3-11.

Frank Lloyd Wright once said, "An expert is a man who has stopped thinking." In unionized shops the relative importance of seniority has always been greater than in nonunion organizations. Recently there has been new emphasis placed on the importance of ability and compromises even in unionized organizations, with many organizations now using a formula which provides more or less equal consideration to seniority and ability. Many contracts are even being written to allow exceptions for those employees who are "head and shoulders" above their contemporaries in terms of ability.

In general, promotion decisions ultimately determine who will make the key decisions within the organization. At stake is the quality management of the organization. Remedying a mistake in the promotion process is a very difficult and expensive procedure and could result in serious decay or destruction of organizational efficiency. The initiative for promotion must belong to the managers and it is their responsibility to see that worthy personnel are promoted. It is the employees' responsibility to qualify for promotion.

Who to promote should be decided by the manager on the basis of his knowledge of the employee's past performance and, more important, a judgment of the employee's capability to perform in a position of higher responsibility. Promotions should be fairly and capably used to place in each job the most competent and productive employee available. Promotions should be a reward only to encourage those employees who make a successful effort to increase their knowledge and skill, maintain a high level of productivity, and demonstrate a capacity to perform in a job of greater responsibility. It should not be necessary to stress that promotions made on the basis of performance should not concern race, sex, religion, national origin, or age.

The cure is not easy, since the time-in-grade syndrome has been ingrained into the system for

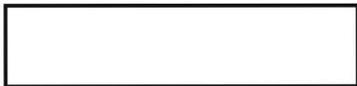
so long. It must be made apparent to everyone that performance and capability will be the primary promotion criteria. Peripheral areas which may serve as indicators (such as education, training, and any professionalization certifications obtained) must be considered, but only as an extension of the primary factors of performance and capability. Time in grade should never be considered since an employee should not be nominated for promotion unless he or she has fulfilled the minimum requirements.

To ensure that this system works and to protect the managers against any charges of discrimination, some basic changes in the method of preparing promotion recommendations must be made. When a deserving employee has attained the minimum time in grade to be considered for promotion, a record of that person's previous performance and a statement of his or her projected capability, together with supporting data pertaining to education, training, and professionalization, should be submitted through the existing promotion channels. Each recommendation should be identified by an arbitrary designator, without any references to name, age, color, sex, time of service, or, most important, time in grade. The selection panel would then be able to make their choices solely on the important performance indicators, thus eliminating one of the major causes of the time-in-grade syndrome. Likewise, job assignments should be made on ability, considering grade if necessary, but not eliminating obvious choices simply because of their grade.

Naturally these two changes are going to cause much discussion and certainly some of those ingrained with the time-in-grade syndrome are going to be upset. This is normal when making any change in behavior patterns. In the long run it should improve the Agency's operations and efficiency, with the resultant cure being worth the bitter pill that must be swallowed.

### A LITTLE T.A. PROBLEM

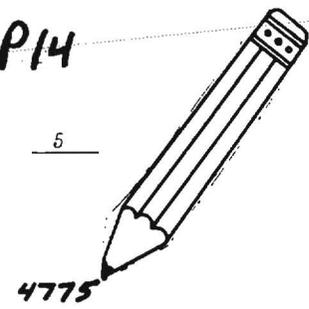
These radio frequencies have been recovered on the Third Army network. Recover the system of generation and allocation.



P14

P.L. 86-36

Address	Unit	1	2	3	4	5
518	3rd Army	4716	4051	4796	—	—
011	15 Inf.Bde	4691	4116	4876	4281	—
176	38 Inf.Bde	4762	4237	5012	4327	—
234	420 Arty.Reg.	4898	4303	4023	—	—
469	796 Sply.Reg.	5041	4356	4161	4606	—
853	562 Inf.Reg.	4085	4505	4305	4750	—
503	87 Inf.Reg.	4165	4610	4330	—	—
217	149 Inf.Reg.	4241	4686	—	4766	—
004	281 Inf.Reg.	4280	4690	4420	4875	—
606	356 Inf.Reg.	4370	4805	4620	5055	—
180	618 Inf.Reg.	4438	4893	4683	—	—

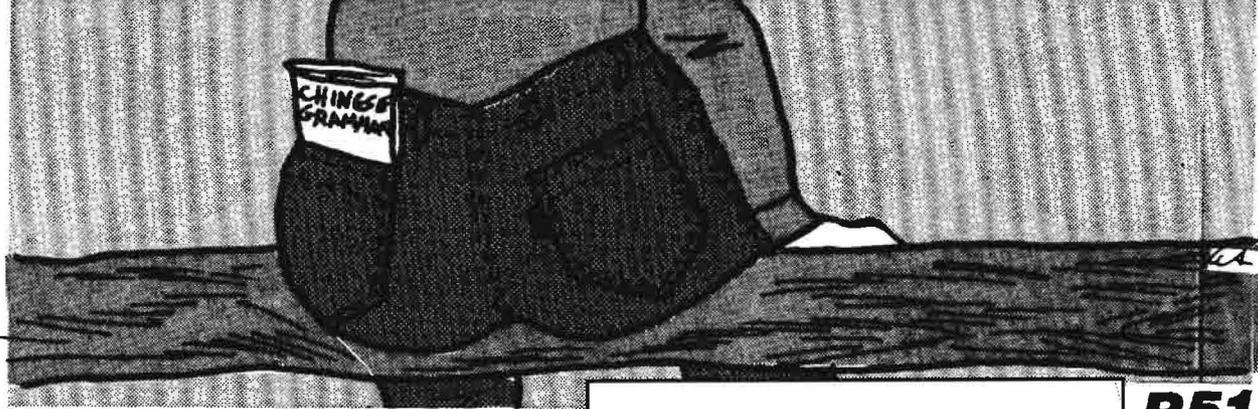


Solution next month.

(U)

UNCLASSIFIED

# BACKING INTO LANGUAGE ACQUISITION



**R51**

In this paper, as in the 5 May 1977 SIGLEX talk on which it is based, I try to illustrate the relative ease for the mathematically literate (in English) to acquire analogous literacy in some foreign (i.e. non-English) language. In mathematics (mostly) and in many (not all) of the so-called "hard" sciences (frequently), the speaker (writer) *must* say a specific something, and the appropriately literate audience (reader) *knows* what that specific something is. This foreknowledge does not remove the necessity of learning the syntactic essentials of the foreign language, but it can facilitate the task to a significant degree. With more and more worthwhile material in mathematics (electronics, physics, biology. . .) appearing in the open literature in such languages as Russian, Chinese, Japanese, and even such has-beens as German, the working mathematician, engineer, etc., might do himself a service in obtaining at least minimal competency in reading the relevant material. Even were it possible -- and inexpensive -- and rapid -- to obtain a relatively good reliable translation of the original material, the translator himself (perhaps "herself," never "itself") would have to be at least minimally competent in mathematics, engineering, etc. I suspect that it's much easier for the ordinary mathematician to learn to read in Russian about mathematics than for the ordinary Russian linguist to learn to read about mathematics in any language.

My few examples are all from an area of elementary mathematics, that of the theory of equations, and, specifically, the mathematical construct called a "polynomial" (see Fig. 1).

$$ax^n + bx^{n-1} + \dots + cx + d$$

(degree n)

$$5x^3 + 2x^2 + 17x + 4$$

(degree 3)

Fig. 1. Polynomial

The word component "-nom-" has the meaning "name" or "term." Hence, "binomial" refers to an expression that has two terms, "trinomial" to one that has three terms, etc. Fig. 2 sketches the etymology, in English, of the word "polynomial" and also shows its equivalent "names" in Russian and Chinese.

polynomial	<u>МНОГОЧЛЕН</u>	多項式
("many terms")	("many-term")	("many term expression")

Fig. 2. Etymology of "polynomial"

When two polynomials are multiplied together, as shown in Fig. 3, the result -- another polynomial -- is called the "product" of the first two.

$$(ax^5 + \dots)(bx^3 + \dots) = abx^{5+3} = abx^8$$

Fig. 3

A fact, well known to the mathematician, is stated, in Russian, in Fig. 4, mostly to suggest how the Russian handling of the "double negative" can be made more palatable to the mathematician by an example where he *knows* that the *English* sentence has a single negative.

Произведение	многочленов,	отличных
[[the] product]	(of polynomials)	(different)
от нуля,	никогда не	будет
(from) (zero)	(never) (not)	(will be)
равным нулю.		
(equal) (to zero)		
= "will never be"		

Fig. 4

UNCLASSIFIED

UNCLASSIFIED

Another glance at Fig. 4 might help recall that the degree (largest exponent) of the product of polynomials is equal to the *sum* of the degrees of the polynomials being multiplied. That's precisely what is being said in Figs. 5 and 6, except that Fig. 6 insists that the two polynomials be "non-zero."

Степень	произведения	двух
([the] degree)	(of [the] product)	(of two)
многочленов	равна	сумме
(polynomials)	([is] equal)	(to [the] sum)
степеней	этих	многочленов.
(of [the] degrees)	(of those)	(polynomials)

Fig. 5

两个	非零	多项式	的
(two)	(non-zero)	(polynomial[s])	('s)
积	的	次数	等于
(product)	('s)	(degree)	([is] equal to)
两个	多项式	的	次数
([these] two)	(polynomial[s])	('s)	(degree[s])
的和。			
('s)	(sum)		

Fig. 6

Having done *some* study of Russian (Chinese) syntax, morphology, lexicology (how to handle a dictionary when the alphabet is different or, respectively, nonexistent), our mathematician may simply be *reinforced* by examples such as the last two. He might be taught something about Chinese syntax in the next example (Fig. 7), precisely because he *knows* what the sentence is saying and, therefore, will learn, albeit the hard way, what a nice relative pronoun is doing in a place like that.

这个	方程	可能	有
(this)	(equation)	(may)	(have)
D	E	F	G
的	有理	根	是 ±1, ±3, ...
(which)	(rational)	(root[s])	(are)
C	A	B	H
(Letters indicate sequence of translation into English: "Rational roots which this equation may have are. . .")			

Fig. 7

Besides examples of syntactic behavior, the mathematician is likely to run into other examples of (foreign) linguistic cavortings where he is almost uniquely equipped to determine the unique exegesis. The German four-letter "abbreviation" (a growing unpleasant phenomenon world-wide) in Fig. 8 presented some difficulty until the German clues (nouns begin with capital letters) combined with the translator's knowledge of what mathematicians *always* say in such instances. Fig. 9 shows the standard (and idiosyncratically mathematical) renderings in English, Russian, and Chinese, plus some additional hints of "morphological" behavior in the four languages at issue.

Sei o.B.d.A. m = 1.
(let) ( ? )

Fig. 8

ohne	Beschränkung	der	Allgemeinheit
(without)	(limitation)	(of)	(general-ity)
не	ограничивая	общности	
(not)	(limiting)	(general-ity)	
不	失	一般	性
(no)	(lose)	(general	-ity)
"with no loss of generality"			

Fig. 9

Another way in which mathematicians can back into language acquisition is by recognizing, in a foreign transliteration, names that they are already familiar with. For example, the name of the French mathematician Hadamard (b. 1865) is spelled in Russian as **Адамар** because neither the H nor the D is pronounced in the original name<sup>1</sup>. The transliteration of Western

<sup>1</sup>The rules for transliterating words and names from 18 languages into Russian are given in the book: Р. С. Гиляревский, Г. А. Старостин, **Иностранные имена и названия в русском тексте** (Foreign Names and Designations in Russian Text), a copy of which is available in the P1 Language Library, Room 3W076.

words and names into Chinese is complicated by the fact that the process involves characters which can be interpreted either according to their *meaning* or according to their *sound*. Fig. 10 shows this two-faced compoment of the character 馬 ("horse"). Note that the Chinese also drop the R from Hadamard's name.

馬 MA ("horse")		
<i>Character used for meaning</i>		
海	馬	
("sea")	("horse")	→ "sea horse"
河	馬	
("river")	("horse")	→ "hippopotamus" <sup>2</sup>
<i>Character used for sound<sup>3</sup></i>		
馬	達	
MA	DA	→ "motor"
("horse")	("arrive")	
馬	克	思
MA	KE	SI
("horse")	("overcome")	("think")
費	尔	馬
FEI	R	MA
("expense")	("you")	("horse")
阿	達	馬
A	DA	MA
(no sep- arate meaning)	("arrive")	("horse")
→ "Hadamard"		

Fig. 10

Finally, Fig. 11 exhibits another frequent trick in modern languages, the neologism obtained by concatenating the original characters (sometimes syllables) of consecutive words. To reconstruct the original string of words, one needs to know that neologisms are sometimes formed this way, one needs to be knowledgeable in the field in question, and, occasionally, one has to be lucky.

<sup>2</sup>Which, strangely enough, is derived from Greek words meaning "river horse."

FORTRAN	<	formula translator
GESTAPO	<	Geheimstaatspolizei
матрб	<	математическое обращение
		("software," not literal translation "mathematical processing")

Fig. 11

Certainly, acquiring proficiency in reading any foreign language is not easy. However, it may be easier than you think. It may also be more necessary than you think. It might also be fun.

<sup>3</sup>Sometimes, when transliterating a foreign word or name, a particular Chinese character will be selected for its sound and also its meaning or connotation. Hence, the character 馬 would be particularly appropriate in transliterating, say, the name of a British cavalry officer. In PI's *Quarterly Review for Linguists* (February 1972) [redacted] said, "It was recently brought to my attention by a British friend, [redacted] that the Chinese term for that venerable cocktail, the martini

P.L. 86-36

P.L. 86-36

馬提尼 could have been more imaginatively written as 馬踢你 (also pronounced MA-TI-NI, but meaning 'horse-kick-you').<sup>3</sup> Actually, although the Chinese transliteration is standard, some Chinese do appreciate the "horse-kick-you" pun. There is at least one other transliterated foreign word in which the sound of a syllable got confused with the meaning of the Chinese character used to represent it. According to *Aspects of Chinese Sociolinguistics: Essays by Yuen Ren Chao* (Stanford University Press, Stanford, 1976, p. 398), "In the Shanghai tramway system the cars did not run all night and passengers going out nights would naturally be interested in the last cars on various lines. . . . But the penultimate car was also of practical importance." According to the essayist, the folks in Shanghai transliterated the British pronunciation of "last car" by three Chinese characters, roughly pronounced, in Shanghai, LA SI KA. Since the middle character, in addition to having the sound SI, also has the meaning "four," and the number before four is "three" (the Chinese character for which is pronounced SAN), the obvious move, at least in Shanghai, was to list both the last car (LA SI KA) and the next-to-last car (LA SAN KA).

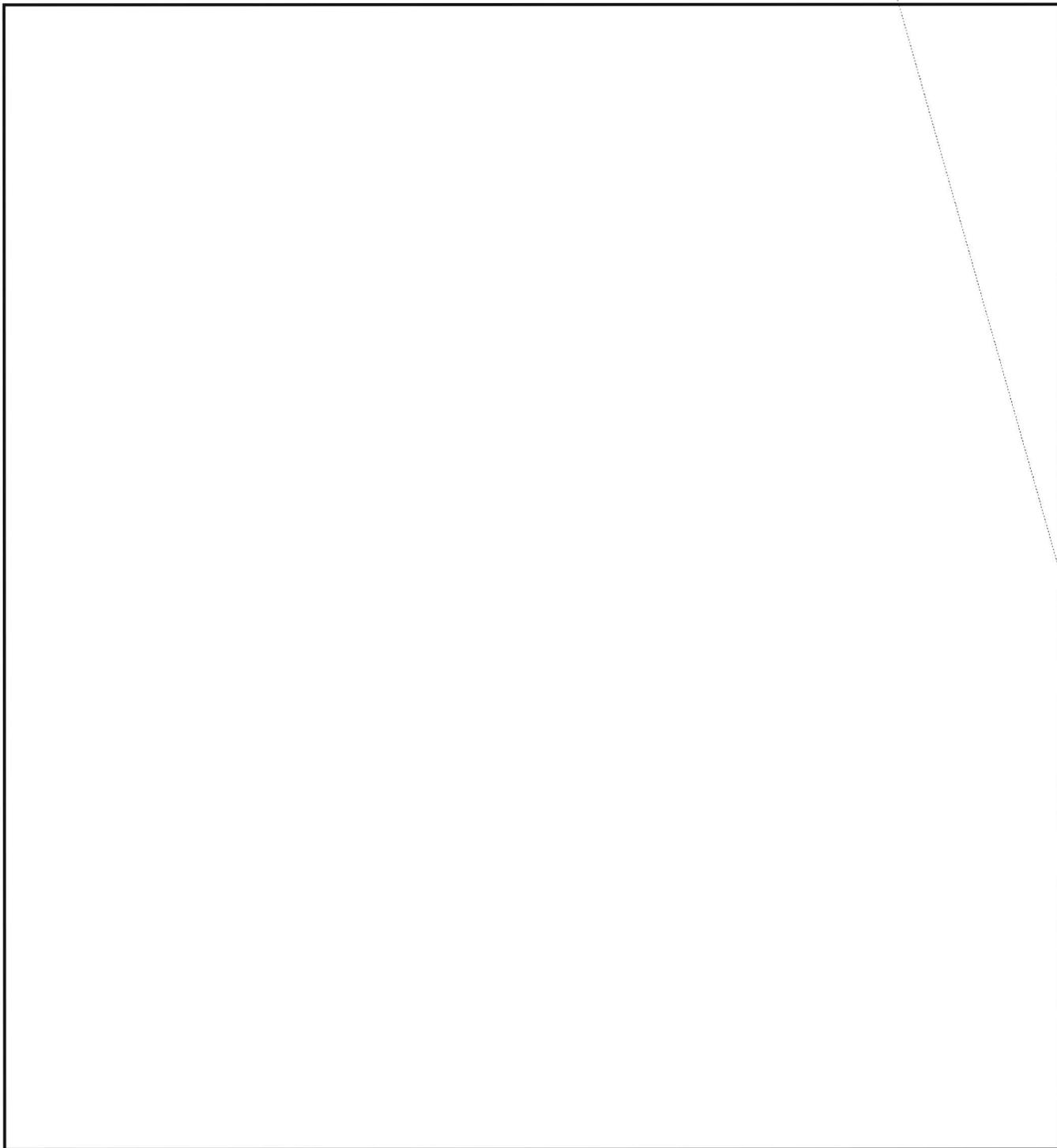
# **NSA-crostic No.10**

By A.J.S.

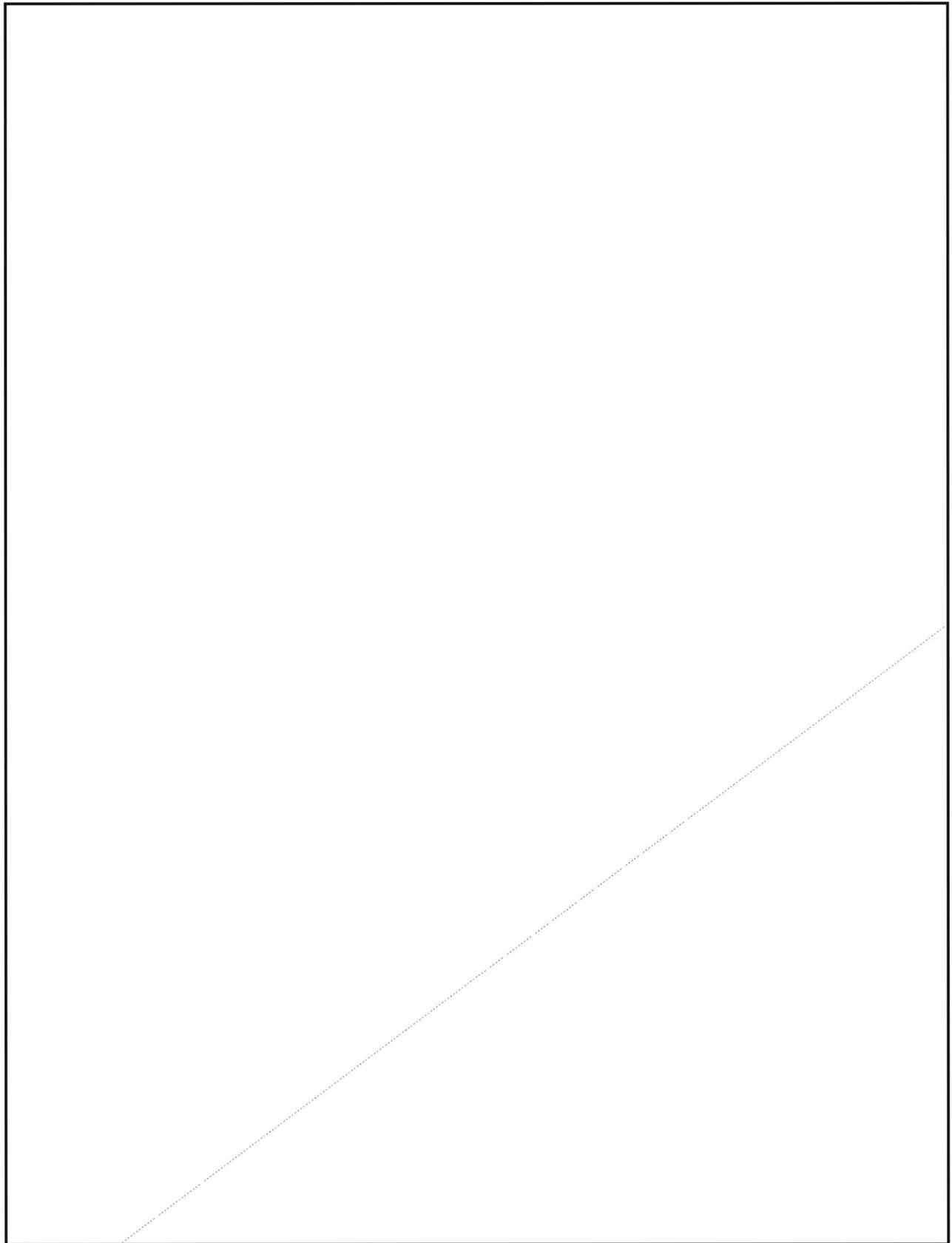
*The quotation on the next page was taken from the published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.*

DEFINITIONS

WORDS

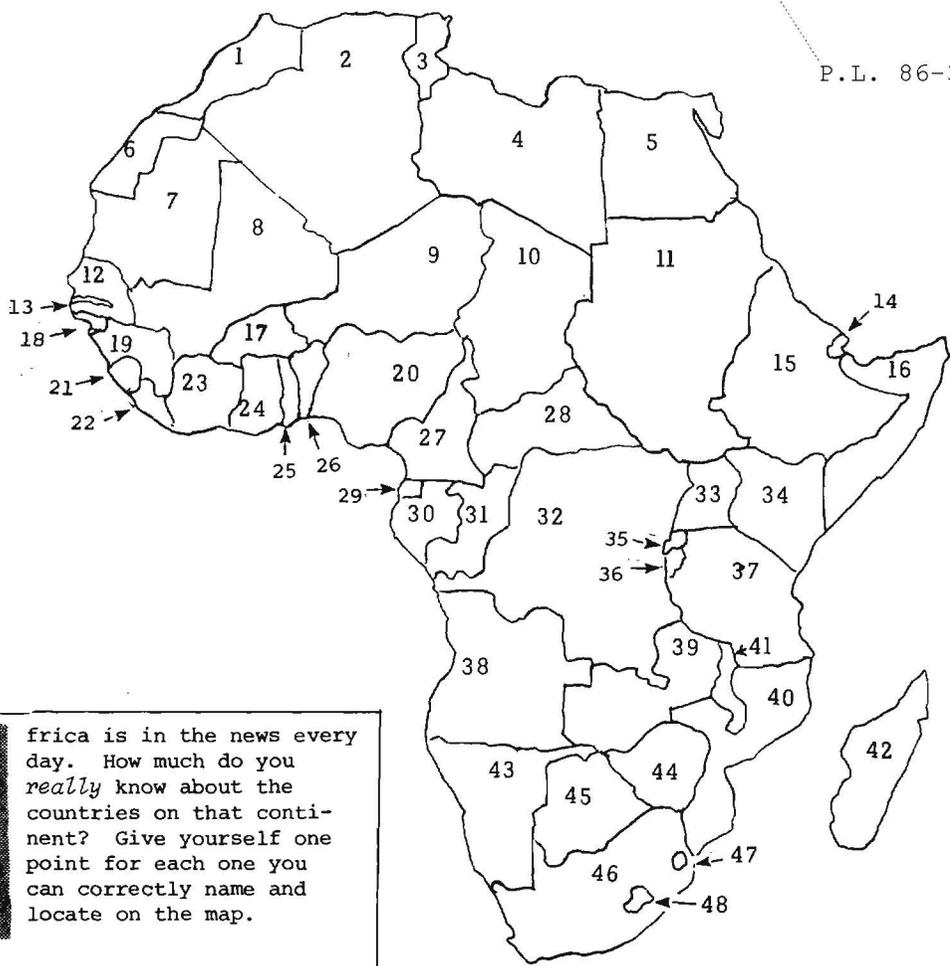
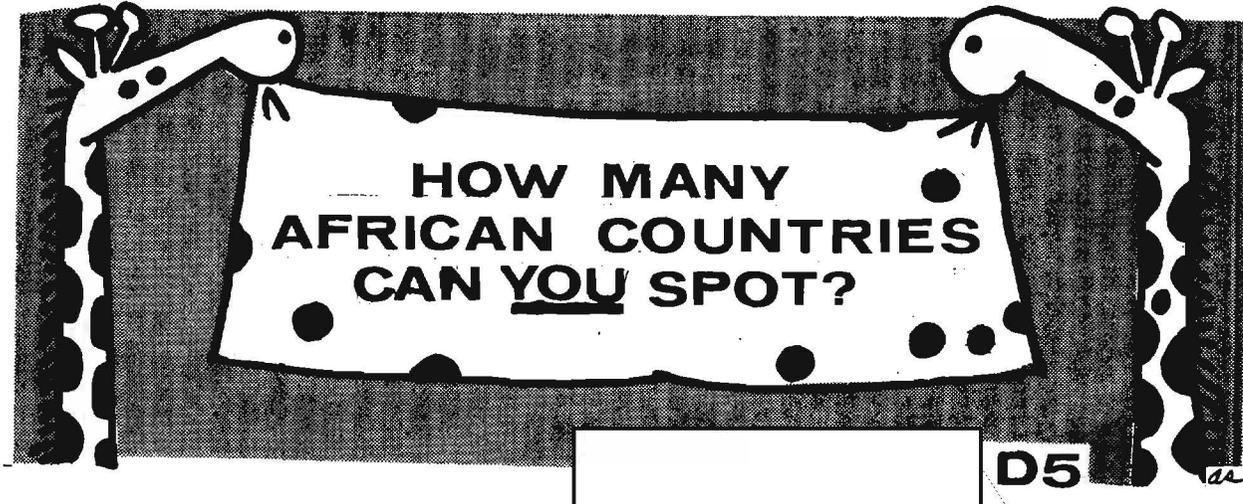


**UNCLASSIFIED**

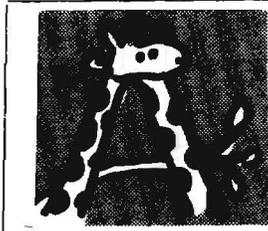


*(Solution next month)*

**UNCLASSIFIED**



P.L. 86-36



Africa is in the news every day. How much do you *really* know about the countries on that continent? Give yourself one point for each one you can correctly name and locate on the map.

- 0-8 Very poor!
  - 8-12 Not too bad
  - 12-16 Getting better
  - 17-20 Excellent
  - Over 20 If you didn't cheat, you're in the genius category!
- (Answers on page 20)

UNCLASSIFIED

# LANGUAGE PROCESSING FORVM

[redacted] P xvi  
[redacted] P xvi

**L**anguage processing has undergone many changes at NSA as a result of such varied pressures as re-organizations, increases and decreases in personnel, and the influences of data-processing procedures. Changes in technology and target-country practices, as well as shifting policies and priorities, have placed requirements for flexibility upon a discipline which by its nature responds slowly to change (language acquisition is a time-consuming process).

In order to keep pace with rapidly changing demands, good communication is essential. To provide a central focus for persons in various elements, PI has inaugurated a LANGUAGE PROCESSING FORVM. Meetings of this forum feature speakers and discussion on a focus topic. Audience participation is encouraged in order to obtain views, opinions, and information about successes and failures from a broad sample of persons actively engaged in language processing.

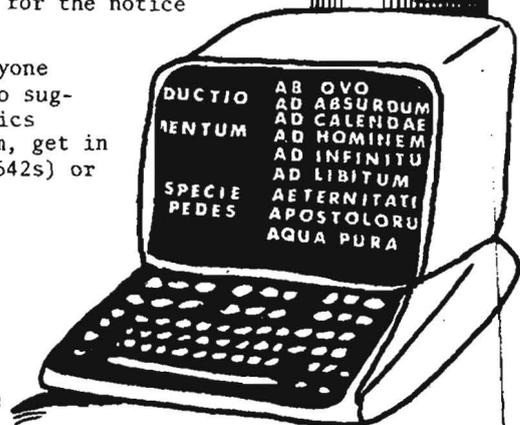
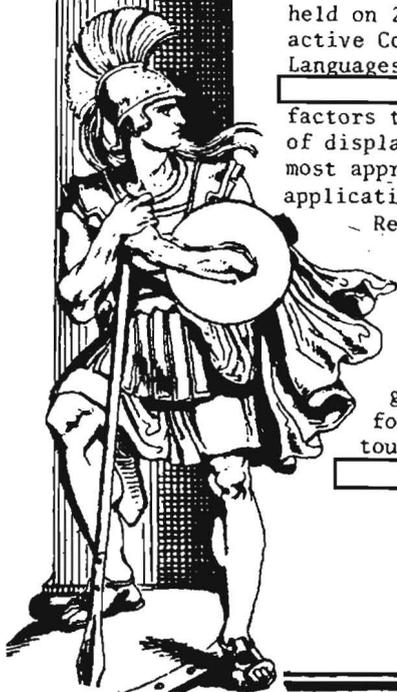
Minutes of each forum meeting, including suggestions, recommendations, criticisms expressed, and language-processing requirements resulting therefrom, will be distributed to a mailing list of interested persons and to all managers of elements having potential interest in the topic discussed.

The impact of CRT (cathode-ray tube) technology upon language processing provides the content of at least the first two meetings. The first of these, which was held on 28 October, was titled "The Impact of Interactive Computer Graphics on the Processing of Ideographic Languages." A panel consisting of [redacted]

[redacted] led a discussion focusing on factors that must be considered in choosing which type of display system (full-graphics or alphanumeric) is most appropriate for a given [redacted] processing application. The second program, "Is an Interactive CRT Really the Answer (And, If So, What Was the Question)?", is planned for late November or early December. Look for the notice giving time and place.

Attendance is open to anyone interested in the issue. To suggest language-processing topics for consideration by the forum, get in touch with [redacted] (P16, x5642s) or [redacted] (P16, x4032s).

P.L. 86-36



DUCTIO AB OVO  
AD ABSURDUM  
AD CALENDAE  
MENTUM AD HOMINIEM  
AD INFINITU  
AD LIBITUM  
SPECIE AETERNITATI  
PEDES APOSTOLORU  
AQUA PURA

UNCLASSIFIED

# C.A.A. NEWS

P14

COMMUNICATIONS ANALYSIS ASSOCIATION

## CAA Board:

President-elect: [redacted]  
Treasurer: [redacted]  
Secretary: [redacted]  
Board members: [redacted]

David Gaddy, 52475

## November presentation:

All you ever wanted to know about [redacted] what's really happening [redacted] (and vealed by [redacted] will be re- Watch for the notices.

"So here I am a professional! Now what? Where do I go from here?" That's a good question. [redacted] mentioned postprofessional development in his letter, published here last month. What do you think about it? What should we be doing about it? Or do you care, one way or the other? The CAA Board is beginning to think about maybe having a round table discussion about postprofessional development, sometime after the first of the year. Are you interested? If you are, then send a note or call a board member and tell us what you think.

## Membership drive:

Some of you folks out there have always wanted to be a member of the CAA but you just haven't known how to go about joining -- isn't that right? Well, anyway, now is the time to join. Come to one of our presentations a few minutes early. Or call one of the board members. If you don't have a phone -- write (to me). Dues are \$1.00 per year.

Did you attend the September presentation by Whitney Reed ("Doing It Remotely"), which described his experiences in developing and managing the B Remote Operating Facility? If you did, did you remember to sign up for that special tour of BROF?

## It rhymes with "tickle"

I hardly know where to start. The Five-Foot Shelf of Great Cryptologic Literature (abbreviated FFSGCL and pronounced "foffs-gickle," for all those who *have* to pronounce abbreviations) actually exists. A large box arrived in my office not long ago, containing two large notebooks chock full of interesting reading about COMSEC -- courtesy of Harry Daniels and [redacted]

These books contain a series of lectures on COMSEC by David G. Boak, as well as surveys and examples of current systems and equipment, and lots of other interesting goodies. You can find these books (as soon as I finish reading them) on the *shelf* in the Cryptologic Collection of the P1 Technical Library, Room 3W076. [redacted] 4017s, can help you find the shelf. Among the books that have been suggested by other people are: Sinkov, *Cryptanalysis*; Kahn, *Codebreakers*; Blair, *Silent Victory*; Pratt, *Secret and Urgent*; H. F. Gaines, *Cryptanalysis* (Dover); L. D. Smith, *Cryptography* (Dover); Winterbotham, *Ultra Secret*.

The point of the shelf, you will remember, is that each item describes the activities of a skill field to people *outside* that skill field (i.e., in other cryptologic skill fields).

Not everyone agrees about what should be on the shelf. Some people are themselves aggressive seekers of information about what's going on in other people's territories, and these people were quick to share with me where they find their information (Project Management

Directives, journals and periodicals of the services and the SCAs, DDT's *TeleCOMMENTS*, etc.). But far too many people in our business spend most of their energy just keeping up with what's happening in their *own* field. Reaching *this* audience when writing about some *other* field isn't easy -- I don't think it happens nearly as often as many authors think it does. Most cryptologic writing, unfortunately, is aimed at "insiders" -- not just people inside cryptology, but, rather, the people inside the writer's skill field.

"Can you tell me a little more about what you do?" "Didn't you read my article/report/paper? It's all there in black and white!" "Yes, I read it. That's why I'm calling. . ."

Think back over what cryptologic writing you can remember that made an impression upon you, where the subject was outside your own field or pet project areas. How many different writers (or articles/reports/papers) can you recall?

It's not easy to write about your favorite subject in such a way that an "outsider" will completely understand you and sense your enthusiasm. If you take this statement as a personal challenge, try doing it and send in your article to CRYPTOLOG. It's just the sort of thing that CRYPTOLOG was set up to publish.

By the way, Dave Gaddy now claims that the five-foot shelf wasn't his idea after all! (I think he just doesn't want to find out how we will pronounce DGFFSGCL!)

UNCLASSIFIED

# WHAT EVER DOES "HOWEVER" MEAN?

**G03**

**E**nglish adverbials are poorly understood by most writers, whether they be innovative writers, report writers, or translators. The difficulty is greatly enhanced for translators if they tend to look upon lexical items in a foreign language as having one-for-one "word" correspondences in English, i.e., they have a once-a-word-always-a-word mentality. The function of the word is oftentimes more important than its gloss -- its so-called meaning or equivalent.

As an example, let us take the English lexical item "however." Writers and translators have great difficulty with this word. They have been exposed to teachers or books maintaining that "but" cannot initiate a sentence, much less a paragraph, and must be replaced by the more elegant "however." Then, too, their sources stress that words such as "however," "nevertheless," etc. must be set off by commas. But see page 49a of *Webster's Third New International Dictionary* for usage of the comma with transitional words and expressions (i.e. adverbials):

"4.1.3. Commas set off transitional words and expressions (as *on the contrary, on the other hand, consequently, furthermore, moreover, nevertheless, therefore*) whenever they are or would be spoken with the adjacent rising or sustained pauses that indicate subordinate matter. 'The question, however, remains unsettled.' 'Nevertheless, we shall go.' 'On the contrary, under the rules a vote is in order.'

"4.1.3.1. Such expressions may occur in context so as to be spoken without significant pauses and may likewise require no punctuation. 'We shall therefore proceed with the operation.' 'The weaklings will consequently be forced to drop out.' 'A clear-cut decision is on the other hand too much to expect.'"

The translator has the added difficulty of the fact that oftentimes a number of words in the foreign language can be translated as "however" in English. But oftentimes the dictionaries label the foreign word as some given part of speech in that language and then give English glosses which are not the same part of speech in English, and this does become confusing!

So, let's take a look at this English word "however." What part of speech *is* it? It's a conjunction, a concessive conjunct, and an interrogative. In each function its placement in a clause or sentence and its punctuation are fixed. As a conjunction, "however" is a simple subordinating conjunction. It is also one of

the so-called *wh*-elements which are initial markers of subordination in interrogative *wh*-clauses, in relative *wh*-clauses, and in conditional-concessive *wh*-clauses (i.e. *who/whom/whose, which, where, when, whether, how, what, why, whoever, whomever, which ever, wherever, whenever, whatever, however*). "However" is also a concessive conjunct, i. e., it is an adverbial that occurs peripherally in clause structures but is primarily connective in function. Adverbials as a class can occur in four positions in the declarative form of a clause:

- I - initial position (i.e., before the subject)
- M1 - medial position #1:
  - (a) immediately before the operator (DO, etc.), or
  - (b) between two auxiliaries.
- M2 - medial position #2:
  - (a) immediately before the verb, or
  - (b) before the complement in intensive BE-clauses, e. g. "He is soon to be transferred."
- E - end position:
  - (a) after an intransitive verb, or
  - (b) after an object or complement.

Concessive conjuncts are contrastive, i.e., they signal the unexpected, surprising nature of what is being said in view of what was said just before:

"He has been in office for only a few months. He has, *however*, achieved more than any of his predecessors."

But note that when "however" is positioned initially it is sometimes used in conversation to indicate that the speaker wishes to change the subject:

"I think you had no right to speak to him in that way. *However*, I really wanted to let you know what I think about your recent letters to me."

Conjuncts also occur as correlatives reinforcing particular subordinators: "however" is one of eight conjuncts (*yet, still, however, nevertheless, nonetheless, notwithstanding, anyway, anyhow*) that can occur after five concessive subordinators (*although, [even] though, while, granted [that], even if*). "However" as a conjunct (along with the antithetic "then" and "though") can also be linked to a preceding clause by the coordinator "but". "However"

\* In the article "The Legendary William F. Friedman" (*NSA Cryptologic Spectrum*, Winter 1974, Vol. 4, No. 1), Lambros Callimahos mentions that a code message that Mr. Friedman broke started with the words "But though. . ."

UNCLASSIFIED

does not follow the "but" immediately; i.e., it cannot be initial unless there is no conjunction in front of it:

"You can phone the doctor if you like, *but* I very much doubt, *however*, whether he'll come out on a Saturday night."

"You can phone the doctor if you like. *However*, I very much doubt whether he'll come out on a Saturday night."

As a subordinator, "however" can occur in a nominal clause:

Subject: "However the election goes will depend on the situation."

Direct object: "I can't imagine *however* he got into that situation"; "I can't imagine *how* he ever got into that situation."

Subject complement: "The question is not *however* it came up but who will solve it."

Appositive: "My original question, *however* will he go to the Middle East this time, has not been answered."

Adverbial complement: "I wasn't certain *however* long he'd been here."

Prepositional complement: "No one was consulted *in* however small a way."

But "however" more usually occurs as an adverbial clause:

"He is welcome *however* he comes."  
 "However much advice he gets, he does exactly as he sees fit."

Note that in restricted circumstances (namely, with an abstract noun-phrase subject of a subject-verb-complement clause), the verb BE can be omitted from a universal conditional-concessive clause:

"However great the pitfalls (are), we must do out best to succeed."

This particular type of clause can also be treated as an optative subjunctive or as front-placing of the main verb:

"However that may be, he will do his best";  
 "Be that as it may, he will do his best."

"However" is also one of a group of informal intensificatory question-words (*whoever, whatever, whichever, whenever, wherever, however*) but these words are usually spelled as two separate words and thus distinguished from the subordinating *wh*-words. There are various ways of intensifying the emotive effect of a *wh*-question, however:

"How ever did you think of that?";  
 "However did you think of that!"; "How in heaven's name did you think of that?"; etc.

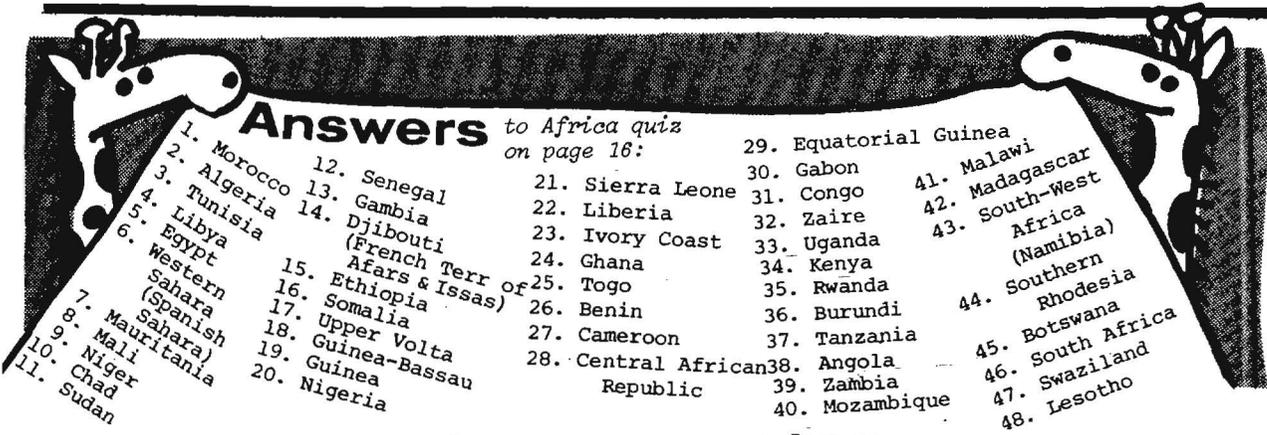
Another use of "however" is for premodification of a maximizer (*fully, thoroughly, totally, completely, perfectly, entirely, utterly, extremely, absolutely*) to form the opening of a dependent adverbial clause:

"However totally they believed in the leader's integrity, they were prepared to examine his actions dispassionately."

Conjuncts in initial position extend the scope of the adverbial to subsequent clauses:

"David doesn't have any money of his own. However, he can ask his parents for some, and he might be able to borrow a small amount from his sister."

This small excursus into the syntax and semantics of "however" is a slight indication of the complexity of adverbials in English and is illustrative of the insights to be gained from a linguistically sound analysis of English. Now, all that remains is to do a similar analysis of the words in some one foreign language that can be glossed as "however"; and, then, do a comparative syntactic and semantic linguistic analysis of this lexical item which is "however" in English and which, in translation from a foreign language, can at times be glossed as "however."



UNCLASSIFIED

# LETTERS

[redacted] recently received the following letter in response to his article "Early Days in NSA Computing" (CRYPTOLOG, August 1977).

Russ:

Congratulations on your fine article "Early Days in NSA Computing." Since I consider myself one of the parents of ABNER, it was especially interesting to me.

It's too bad we don't often get the chance to mention names of people in some of the things we write for publication. An example is the enclosed article "Influence of U.S. Cryptologic Organizations on the Digital Computer Industry," which you may have seen. In case you haven't, I've inscribed this copy. I originally had a long list of names for the acknowledgements paragraph. But since it was written for distribution outside (yes, many things we used to consider classified may now be said out loud!), I was told it would be safer and give less annoyance to those named if we left off the list of names. Some copies have already been distributed, and it's expected the article will eventually have its impact on students of computer history. So I note that you mention [redacted] who indeed did contribute brilliant work on ABNER. Too bad you didn't also recognize Ray Bowman and [redacted] who were really the ones in charge of the engineering. But that's the way with naming names; one doesn't know where to leave off, for fear of leaving somebody out!

As a re-employed retiree, I am working for D4, the people in charge of answering requests under the Freedom of Information Act. My extension is 4656s or, at FANX-III, 8214s. I am starting work on an article about early machines including special-purpose ones (pre-computer), provided the story can be written for uncleared readers. It will be like walking a tightrope, so I'm not sure what good the result will be.

Thanks again for a nice job on ABNER and the 701, etc.

[redacted] D4

*Editor's note:*

The Introduction to [redacted] "Influence of U.S. Cryptologic Organizations on the Digital Computer Industry" (National Security Agency, May 1977, ii + 36 pp., Unclassified) contains the following statement:

"An unfortunate aspect of . . . historical accounts of computer lore is the omission (conspicuously, to some of us) of mention of the National Security

Agency, or of the contributions by that Agency which helped in laying the foundation of the computer industry. The NSA over the years has been required to observe a policy of anonymity, and with good reason. But, in this age of maturing appreciation of the role of computers in nearly all civilized endeavors, it is time for acknowledging that NSA, too, uses computers. In fact, that Agency's contributions to the computer industry have been outstanding. This article relates for the first time some of the details behind the NSA computer story."

P.L. 86-36

[redacted] has told us that he has several extra copies of his article available, and that any CRYPTOLOG reader who would like to have one can contact either him (on 4656s or 8214s) or [redacted] T1213, Room 2N090, 5801s. (U)

In addition to [redacted] letter, which wasn't even addressed to us, we received two genuine Letters to the Editor. Both of them -- hereinafter abridged for reasons of mock modesty -- would like to correct errors of fact.

To the Editor, CRYPTOLOG:

In the article "Expletives Deleted?" (CRYPTOLOG, August 1977), your reference to *sh-/sk-* pairs in English is slightly misleading. It is true that the Greek *skatos* is etymologically related to the appropriate *sh-/sk-* pair in English. However, the true origin of these pairs lies in the Old Norse contributions to English, dating from the period of the Viking invasions of Britain. Typically, in these pairs, such as *skoot/shoot* or *skirl/shrill*, the *sk-* word comes from Old Norse and the *sh-* comes from its cousin in Anglo-Saxon.

[redacted] A542

To the Editor, CRYPTOLOG:

Your contention, in "Expletives Deleted?", that Ferdinand de Lesseps was "creator" of the Panama Canal requires some clarification. It should be realized that this statement is not entirely accurate. If we study canal roots, we find that, although Monsieur's company was successful in developing the Suez Canal, it failed in Panama. (It finally took Yankee ingenuity to "create" it; among those who know canals best, that's alimetary.) De Lesseps these [bleep!] inaccuracies, the better.

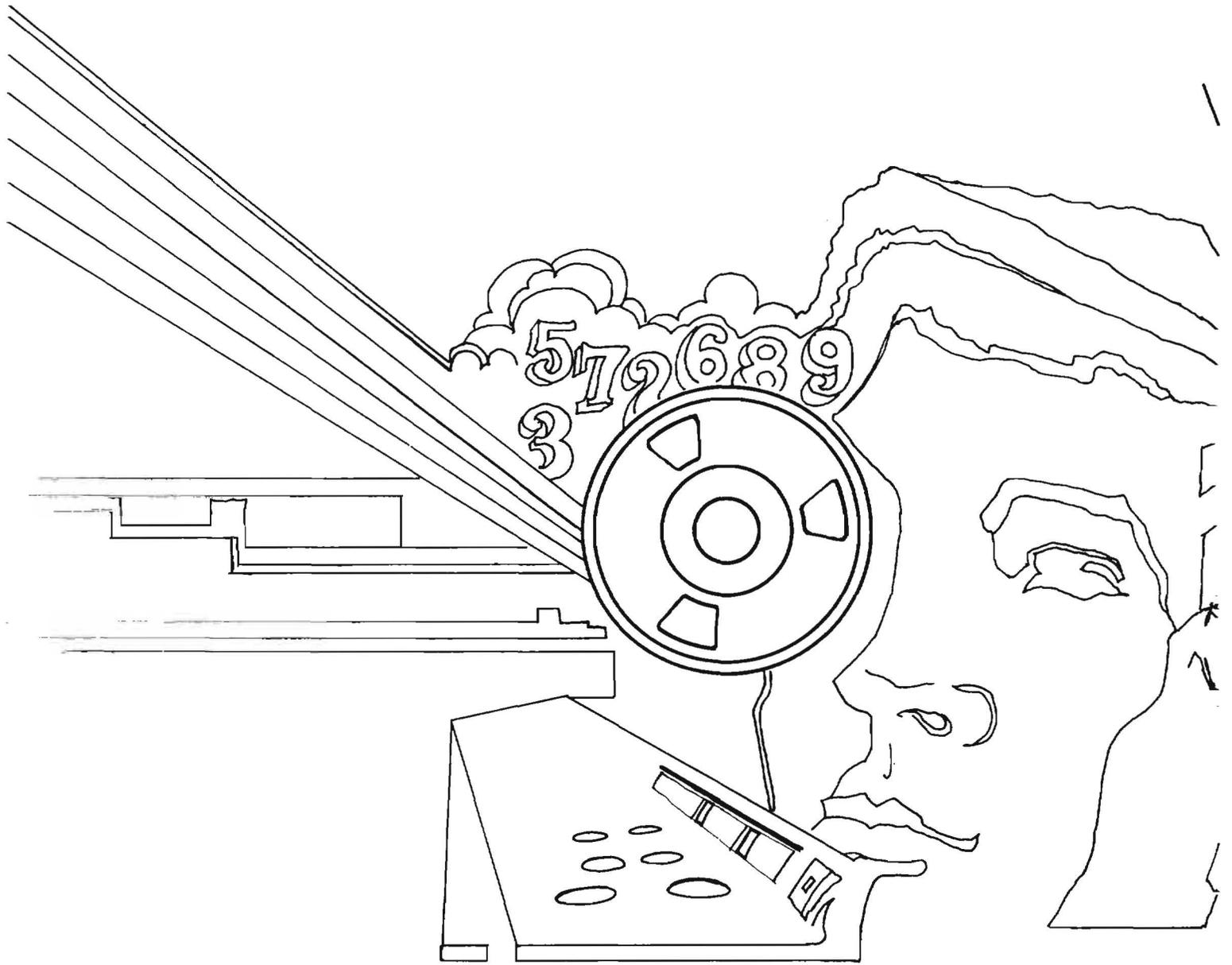
Howard C. Heron, S14

*Editor's reply:*

I'm always pleased to publicize my own mistakes (as I tell my kids, "It proves I'm human!"). I really don't mind these two clarifications at all! Now, if someone had challenged my etymology of the term "raspberry," I would have been completely deflated. (U)

UNCLASSIFIED

~~TOP SECRET~~



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~