



# governmentattic.org

*"Rummaging in the government's attic"*

Description of document: National Security Agency (NSA) Dragon Seeds internal NSA Cryptographic newsletters, 1972-1974

Requested date: 08-April-2013

Release date: 29-July-2022

Posted date: 06-March-2023

Source of document: FOIA Request  
National Security Agency  
Attn: FOIA/PA Office  
9800 Savage Road, Suite 6932  
Fort George G. Meade, MD 20755-6932  
Fax: 443-479-3612  
[Online Request Form](#)

The governmentattic.org web site ("the site") is a First Amendment free speech web site and is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



NATIONAL SECURITY AGENCY  
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 70469A  
29 July 2022

This is a final response to your Freedom of Information Act (FOIA) request dated 8 April 2013, for all issues of the NSA publications entitled "Dragonseeds." As stated in our initial response letter to you, dated 30 April 2013, your request was received on 17 April 2013, and assigned Case Number 70469. There are no assessable fees for this request.

The FOIA allows the public access to federal agency records, except to the extent that such records are protected from disclosure by one of nine exemptions. We have determined that the records you seek are now publicly available and can be obtained by accessing the [www.nsa.gov](http://www.nsa.gov) website and clicking on "Press Room" then selecting "Declassification & Transparency Initiatives," followed by "Internal Periodicals and Publications," and then choosing "Dragon Seeds." Alternatively, you can use the following direct link: <https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/Internal-Periodicals-Publications/#dragon-seeds>.

Since the records responsive to your request are publicly available and we have identified where you can obtain them, we consider your request to be satisfied and, accordingly, your request is being closed at this time. If you need further assistance or would like to discuss any aspect of your request, please do not hesitate to contact me at [foialo@nsa.gov](mailto:foialo@nsa.gov) or you may call (301) 688-6527.

Sincerely,

A handwritten signature in blue ink, which appears to read "Paula A. Gill", followed by the word "for" written in a smaller, cursive script below it.

PAULA A. GILL  
Chief, FOIA/PA Division

~~TOP SECRET~~

# National Security Agency

Fort George G. Meade, Maryland



# DRAGON SEEDS

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~TOP SECRET UMBRA~~

This is Dragon Seeds.

There is fantasy, irony, and the bite of reality in the name. It speaks of the East. And, like the East, it suggests much, says little.

Dragon Seeds is both Mother China and her neighbors. Dragon Seeds is monumental and minuscule. It is the past and future. It begs for elaboration but gives none. In it are echoed softly slurred Mandarin, brittle Vietnamese, determined Korean. In it is the spectre looming over the Thai, Lao, and Khmer. It is frightening and friendly. It is uncertain.

Above all, Dragon Seeds is promise. It is fertile with ideas unbounded, to be cultivated with creativity and imagination. It is challenge. It is alive. It will be more than it is.

Dragon Seeds is yours. May it grow with you.

The Editors

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

PL 86-36/50 USC 3605

DRAGON SEEDS

Publisher

DONALD E. MC COWN, CHIEF B03

Managing Editor

Minnie O. McNeal

Executive Editor

Robert S. Benjamin

Composition

Helen Ferrone

Copy Editor

Thomas L. Glenn

Rewrite Editor

Geraldine J. Pettie

Special Interest Editor

Ray F. Lynch

Biographical Editor

Brooks H. Handy

Education Editor

Marian L. Reed

Feature Editor

Richard V. Curtin

PRESS CORPS

B11 Carolyn Y. Brown

B12 Philip J. Gallagher

B21 Gary Stone

B31 Jack Spencer

Thomas M. Beall

B32 Joe T. Hudson

B33 Louis Ambrosia

B34 Thomas L. Wood

B41 James W. Schmidt

B42 Velma Jefferson

B43 Mary Ann Laslo

B44 Jack L. Thomas

B45 John E. Uzarek

B5 Paul M. Hoagberg

B62

B63 Jean C. Smith

B64 Allen L. Gilbert

B65 Leona B. Dickey

George S. Patterson

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



### TABLE OF CONTENTS

Captain Joslin's Salutation	1
Captain Joslin's Biography	2
Cryptanalysis Through Functional Linguistics..... Donald Lenahan	3
Recovery of a Viet Communist Callsign System.....Wayne E. Stoffel	5
Impact of ARDF on Traffic Analysis..... Al Gilbert	7
The AG-22 and You..... Peggy Barnhill	9
DDP - Dedupe, Delete and Progress..... Charles Swift	12
Chinese Voice: Solution to a Dilemma..... L. St. Clair Myers	14
The Creative Translator.....Tom Glenn	16
Analyzation of Data .....Dick Curtin	19
Seedlings	22
Ask the Dragon Lady	24
Contributors	29

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

**GREETINGS FROM CAPTAIN JOSLIN**

It is my pleasure to introduce to the B Group readership an informal publication which promises to be informative, imaginative, diversified and, yes, even interesting. As I have already stated in my initial announcement of Dragon Seeds to B Group personnel, I am highly enthusiastic about the project and foresee significant returns to the individual. Likewise, I view it as an excellent opportunity for me to become acquainted with you -- to know what you are thinking, to see what techniques you are exploring, to obtain a better feel for what professional problems confront you and those around you, to see what initiatives you are capable of.

Barriers created by the size of B Group, diversity of interests, formality of reports, and the protection of our information have prevented us from communicating easily and sharing fully many concepts and techniques which are professionally exciting and useful to know. Now is your chance for give and take -- to present your thoughts and ideas, to give others the benefit of your particular expertise and experience, or to have your questions answered by the "Dragon Lady," and to find out what others are thinking. I warmly endorse this new B Group venture and encourage your full participation in making Dragon Seeds a provocative, useful, and enjoyable publication.

*H. E. Joslin*

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

CAPTAIN HAROLD E. JOSLIN, CHIEF B

*Captain Harold E. Joslin, USN, brings to B Group the benefit of his 34 years of military service, including a number of key assignments with NSA and the Naval Security Group. Having enlisted in the Navy in 1937, he was serving on Guam as a Second Class Petty Officer in December 1941 when he was captured by the Japanese. (His wife had flown out on the last plane to leave Guam.) After spending 45 months as a POW, he returned to the U.S. in 1945, advanced through the rates to Chief Petty Officer, and was commissioned as an Ensign, USN, in 1946. Captain Joslin is a qualified Interpreter/Translator, having graduated from the Russian Language school at Anacostia.*

*Captain Joslin's career has been highlighted by a number of significant assignments such as Deputy for the Combined Naval Party at GCHQ; Commanding Officer, NSG Activity, Edzell, Scotland; Deputy Director, Naval Security Group Pacific; Assistant Director for Special Operations, Naval Security Group Command; and Deputy Chief of B Group.*

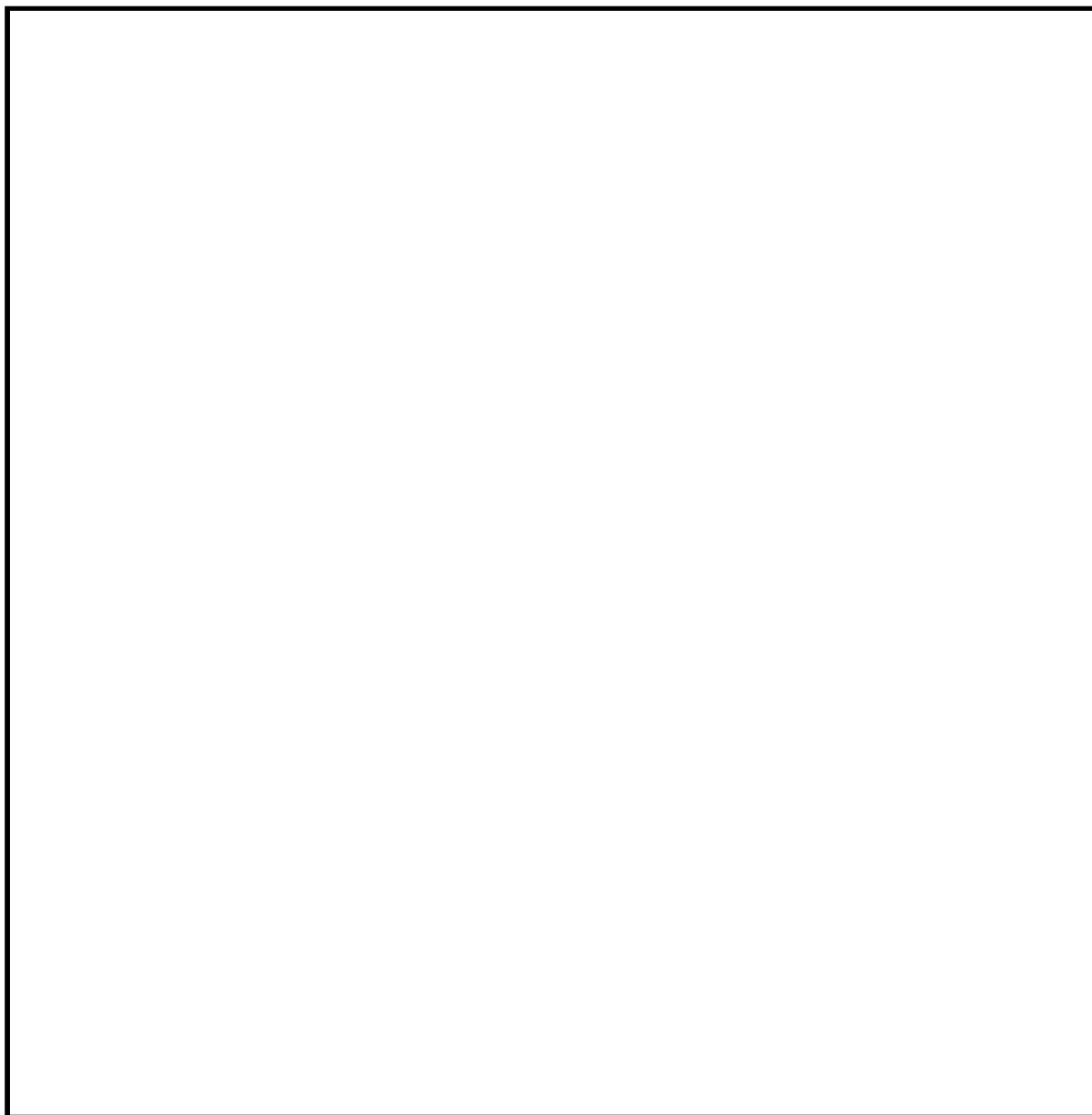
~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

CRYPTANALYSIS THROUGH FUNCTIONAL LINGUISTICS

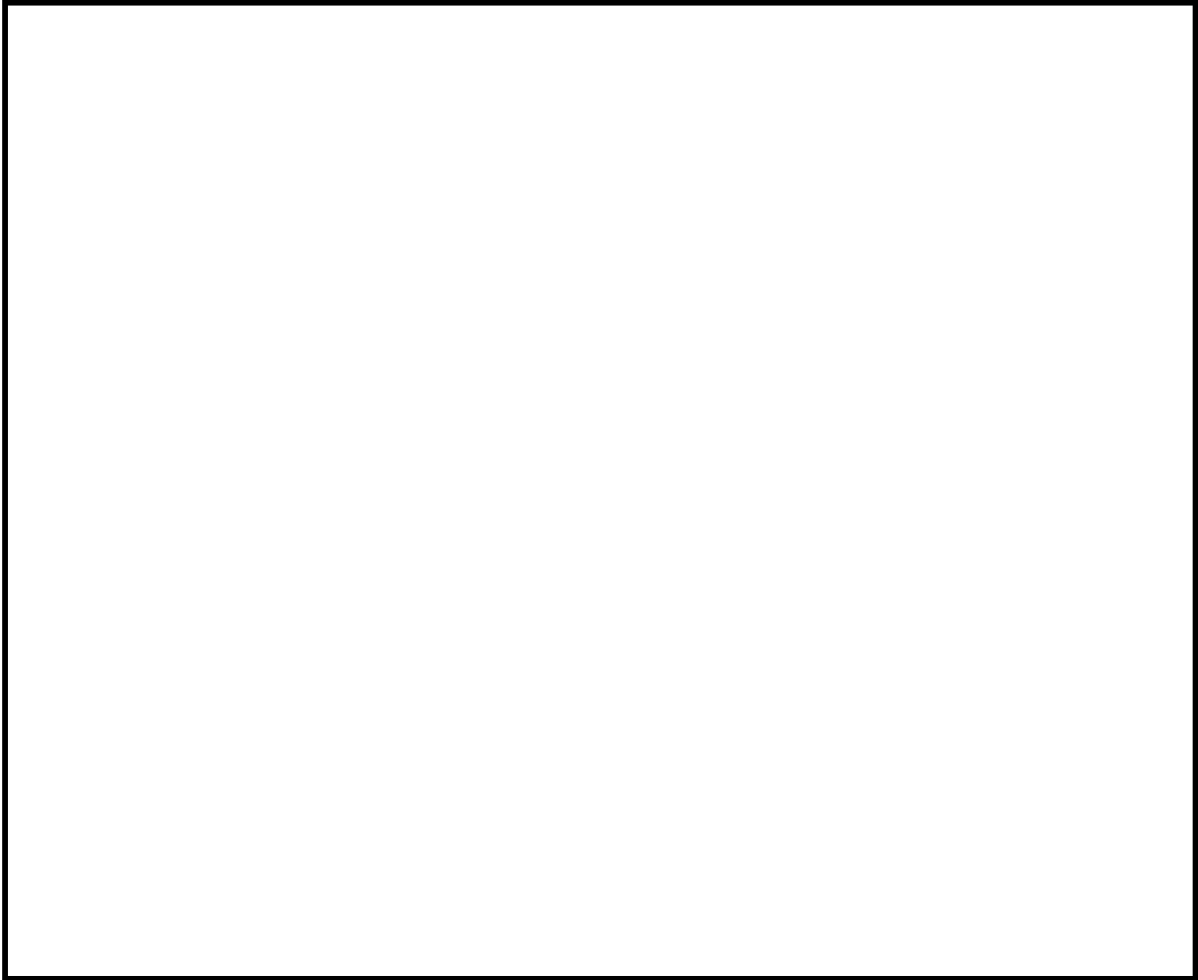
by Donald P. Lenahan, B222



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605



\*\*\*\*

"It's no disgrace to be a slave. It's a disgrace to work voluntarily for someone else."

....Cambodian Proverb

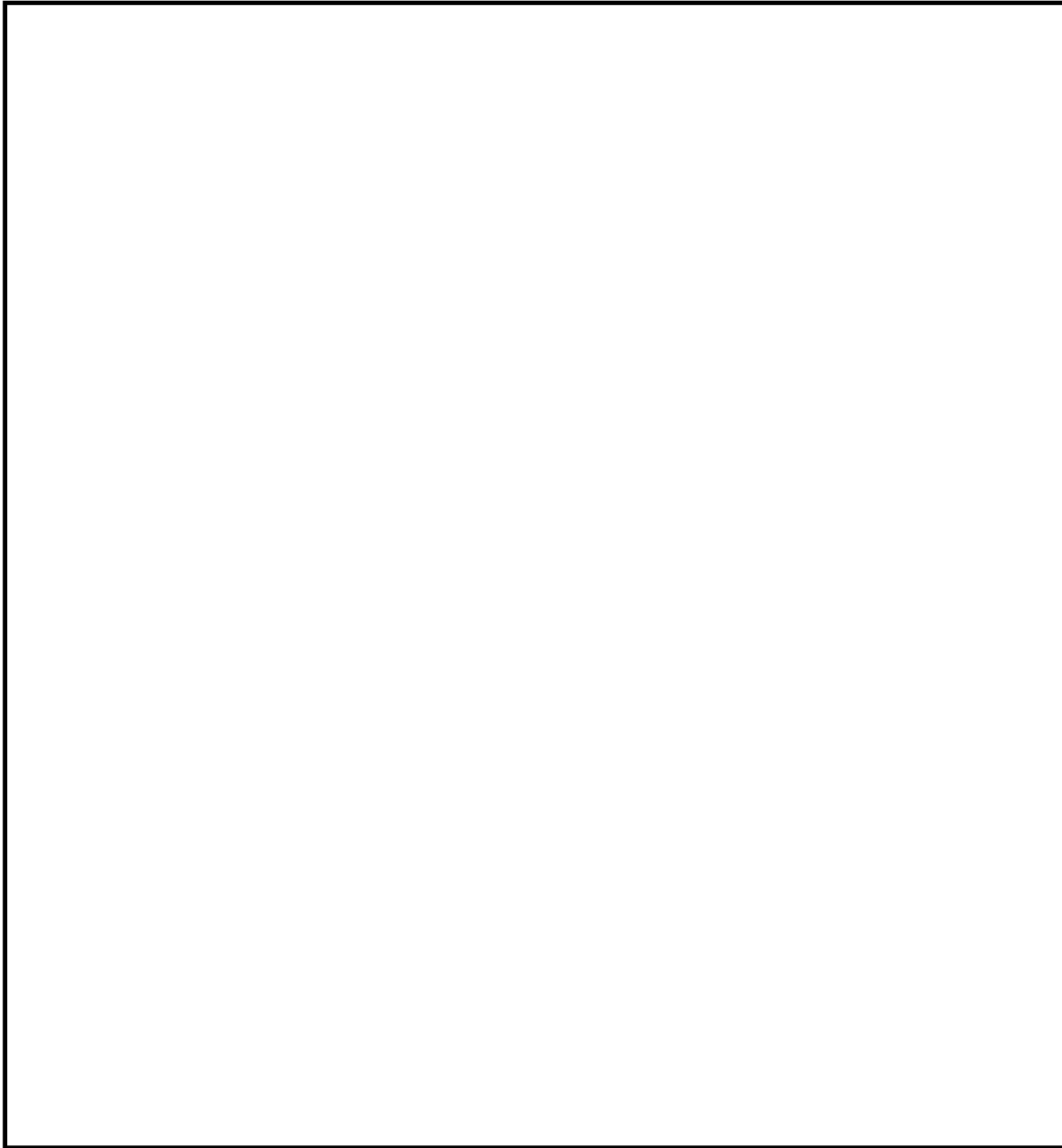
~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

RECOVERY OF A VIETNAMESE COMMUNIST CALLSIGN SYSTEM

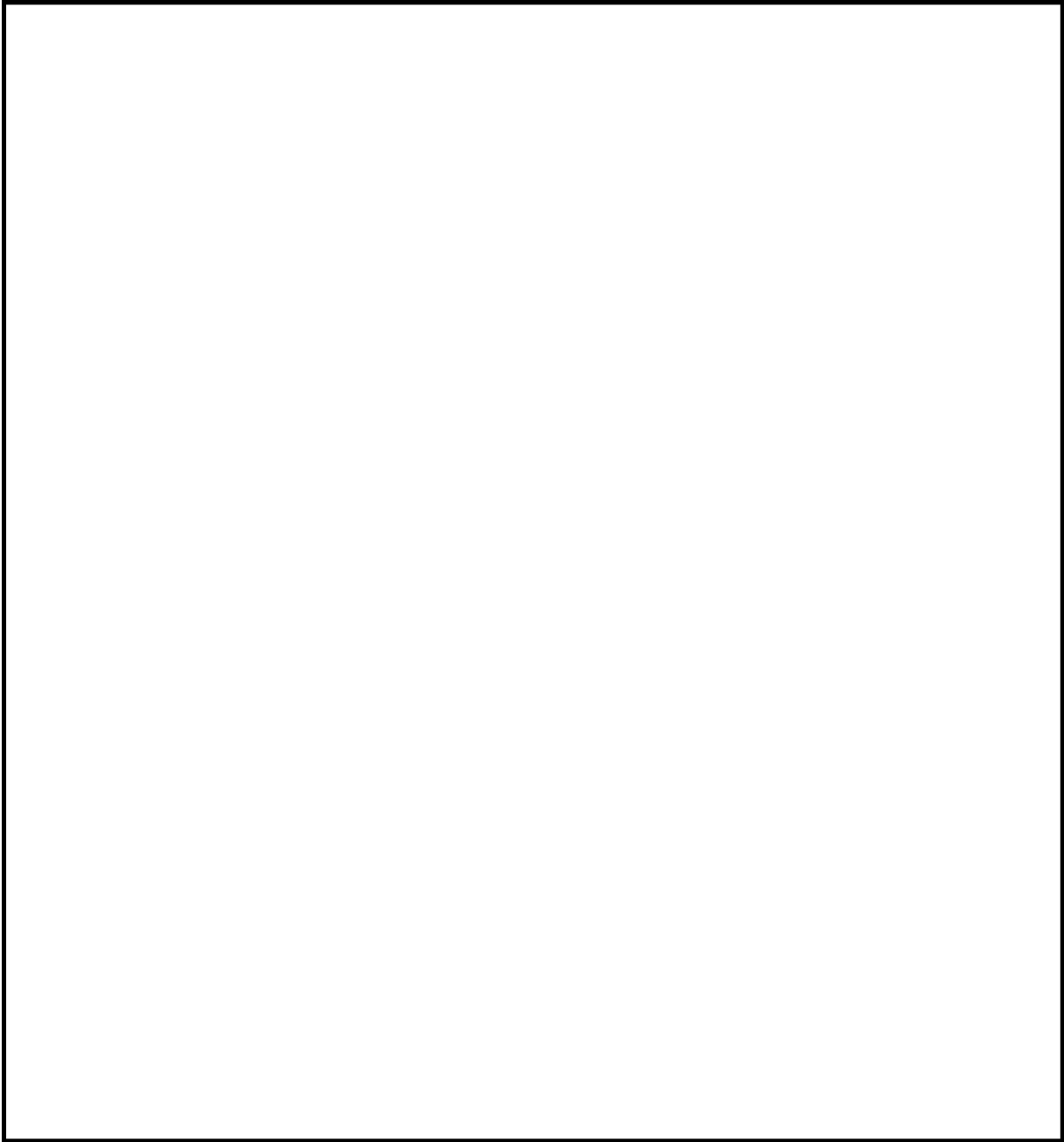
by Wayne Stoffel, B03



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

THE IMPACT OF ARDF ON TRAFFIC ANALYSIS

by Allen L. Gilbert, B6403, 4787s

The Vietnamese conflict and techniques for collection of signal intelligence developed and employed in that arena have influenced the traffic analytic approach to the Vietnamese Communist problem profoundly. One of the most effective techniques employed on a large scale in Vietnam has been Airborne Radio Direction Finding (ARDF). ARDF, in addition to revolutionizing the direct support of tactical units through timely and accurate locating of enemy units, has almost reversed the traffic analytic approach to maintaining continuity and developing new targets in some areas.

Traditionally, the traffic analyst is faced with the problem of reconstructing a communications complex through recovery of callsign and frequency systems, message externals, schedule activity and those rare compromises made by enemy communicators. This route usually requires close scrutiny and cataloging of the elements of intercept through an extended period of time, with the hope that a transmitter location will be compromised or that medium-range direction finding will suggest a location for the activity. ARDF provides a location within a radius of hundreds of meters rather than a number of miles. The availability of ARDF on target transmitters considerably shortens the period of development for new activities and provides almost instant continuity on targets effecting communications changes.

In Vietnam, the concept of ARDF tasking provides coverage in all areas of hostile troop activity. The Military Assistance Command, Vietnam (MACV) controls the tasking of direction finding aircraft and has divided the target area into smaller areas of known enemy activity as reflected by all intelligence sources. Aircraft are deployed to these areas in support of MACV intelligence sources. Aircraft are deployed to these areas in support of MACV intelligence requirements, and therefore direction finding locations are available almost daily on tactical targets. In this process, a certain number of unidentified transmitters are also located. It is apparent that repeated fixing of an

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

unidentified transmitter in the same location, even though the callsigns may change periodically, gives a basis for a suspected continuity, as well as a hint as to the unidentified transmitter in an area where continuity has been lost suggests that the unidentified target represents the lost continuity. When aircraft are deployed to a target area on a daily basis, the recovery of the signal environment in the area builds rapidly.

Certainly, all other elements of traffic analysis must then come into play to establish case notations and identifications and ARDF alone does not solve the problem but what an advantageous beginning it provides!

\*\*\*\*

*People walking along the halls  
People leaning on the walls  
People engaged in conversation  
Or active in clubs for recreation  
With all this action and milling mob  
You wonder who is on the job.*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

THE AG-22 AND YOU

BY Peggy Barnhill, B42

A new item of the SIGINT community's stockpile of electronic gadgets is now installed in sufficient quantity to greatly affect the traffic analytic and processing procedures employed at forward field intercept and within B Group.

The gadget, properly referred to as the "AN/GGC-15" but more commonly called the "AG-22," replaces the typewriters or "mills" previously used by manual Morse intercept operators and radiotelephone transcribers. It consists of an electric typewriter with a modified keyboard, a paper tape punch, and in some cases a paper tape reader, all connected to a solid state station clock, the AN/GSQ-53.

The installation of the AG-22 undoubtedly represents only the first of many revolutionary techniques being developed to permit the rapid transfer of intercepted data from overseas sites to a central processing center. The Improved AG-22 Terminal System (IATS) is already being tested at USM-1, Vint Hill Farm Station, Warrenton, Virginia. As each technological advance is made, changes in traffic handling or processing procedures will occur.

In order to fully understand the impact of the AG-22, it is necessary to examine the equipment and processing developed here at NSA.

The AG-22 produces two outputs. When the operator strikes a key, a character is printed on a page, and simultaneously the corresponding configuration in eight-level code is punched on a paper tape. Thus total intercept is immediately prepared for transmission.

The paper tapes are transmitted via the STRAWHAT data links. There are currently six circuits between NSA and intercept sites in the Far East. These circuits are capable of forwarding data at a rate of 750 and 1500 words per minute.

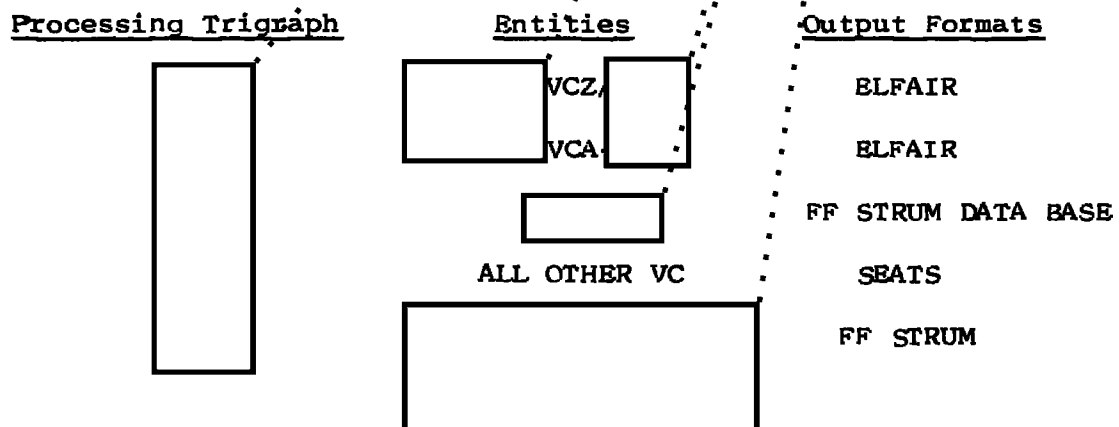
~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

Thus the development of the AG-22 has resulted in the availability to the analyst of total traffic only a few hours after intercept. The data explosion is considerable. During testing on various CHICOM problems 4 to 5.5 times as much data were forwarded and processed as would be expected normally via STRUM or ELFAIR. To make both computer and analyst processing efficient, it was necessary to employ computer techniques previously thought impractical or simply impossible.

All intercept copied on an AG-22, or prepared in an AG-22 compatible format, is processed through the Generalized AG-22 Processing System (GAP) which is a series of IBM 360 computer programs. The GAP system standardizes coding, identifies record types, assigned a processing trigraph based upon case notation, and provides various coverage accounting and quality control listings. Based upon processing trigraphs, GAP data are directed to various subroutine programs. At present there are five user routines operational for B Group problems:



The outputs generated by the user routines are compatible with the existing manually prepared vehicles but may differ slightly in format. Data for B Group entities other than those listed above are directed to LEFTOVER lists which presents traffic in chronological order as copied.

Each of the user routines has follow-on programs which are run prior to the presentation of the data for the traffic analyst -- usually less than 24 hours after intercept. These programs do

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

much of the preliminary data sorting and listing required by analysts. Within the [ ] routine, which has the largest number of users, for example.

1. Callsigns are paged and indicated if predicted for that case.

2. Callsigns are matched against callsigns from all files processed during the last five days. The number of files in which a callsign appeared on the same case will be indicated as well as the number of files in which that callsign appeared on a different case. The differing case will be indicated.

3. Files notated [ ] are matched against all cased and uncased data for the past five days and if possible, reidentified based on callsign usage. If the match is against uncased data, Arbitrary Case Notations (ACN's) may be assigned based on callsign page usage or two-day continuity.

4. Frequencies and schedules are presented in link increments and the reason for each contact break is entered.

5. Preambles are formatted and in some cases traffic type indicators are inserted.

6. Chatter lines are profiled and weighted to indicate significance.

7. Message address information (PAG's, BSD's, etc.) is isolated and presented in a formatted record.

8. Special records indicating call-up order in multiple call-up are generated.

All this is done because analysts and programmers got together and let their imaginations run away with them. The limits of the computer's ability to perform preliminary analysis has certainly not been reached. As we continue to work with the AG-22 and its output, even more capabilities will be defined. Perhaps some day we may even....

Complete this paragraph in 50 words or less and submit your dreams to Peggy Barnhill, B42.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

DDP - DEDUPE, DELETE AND PROGRESS

by Charles W. Swift, B6404

A basic problem that touches every individual in B Group, and probably throughout all Production elements, is the inability to take actions because of missing and misrouted messages. TECHINS 1043 and 1044 provide specific guidance for the routing of information and use of Delivery Distribution Indicators (DDIs) which should assure the proper flow of material; but in practice many problems arise due to a variety of causes.

Instead of seeking out the causes for missing messages, many elements have arbitrarily added DDIs on the theory that if their DDI is on a message they are assured of receipt. Since many DDIs have multiple addressees, this method actually compounds the problem and clogs the machinery designed to provide timely and efficient service to NSA elements.

A recent survey in one B Group office revealed that excess copies of DDP material were being received. One third of the message copies received were tossed away before they reached branch level. Some field stations forwarded technical support messages using DDI combinations that dumped as many as thirty-five copies of the message into the office. At least fifteen copies were tossed away, and only five were really required. Three factors contributed to this situation:

(1) Failure by the field stations to select DDIs according to TECHINS 1043 and 1044. In some instances, the field station had obviously chosen to use multiple DDIs to assure delivery; in other cases the erroneous use had been directed by elements within the office.

(2) Failure to assign qualified and dedicated personnel to distribution functions. Distribution was usually treated as a secondary duty in most elements.

(3) Failure to provide knowledgeable individuals as the focal point for all message distribution problems to assure that distribution personnel at all levels were advised of requirements.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Since "austerity" is the word of the day it would only seem logical that now is the time to isolate costly trouble spots in every facet of operations. We in B Group are in a position to do our part now in respect to the handling of incoming messages. We have started in the right direction by providing for one knowledgeable individual in each office in B to act as the coordinator and authority on all DDI problems, both in-house and field-related. Other actions which should be taken are:

(1) The assignment of qualified individuals to perform distribution functions at all levels.

(2) The constant review and monitoring of DDI requirements by individual elements to differentiate between what is required for job performance and what is just nice to have. The DDI coordinator and the office of primary interest would then be informed of misuses of DDIs and any instances where distribution of material could be reduced or eliminated.

By implementing these procedures a great number of the message copies could be eliminated. This would allow distribution personnel to concentrate more on accurate distribution thereby probably decreasing retransmission requests. A cooperative effort by all elements would relieve the pressure placed on our limited teletype distribution system, thus assisting in the timely receipt and handling of our correspondence.

.\*\*\*\*

"Though the hen may cackle all day, she can lay but one egg."

....from the Burmese

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605CHINESE VOICE: SOLUTION TO A DILEMMA

by L. St. Clair Myers, B441

Let's take a close look at NSA's problems in coping with Chinese voice intercept -- one of the least understood and [redacted] problems in the Agency. Spoken Chinese is without doubt more difficult to grasp than the written language. Native speakers are generally the only ones who can fully perceive the tonal differences and understand the subtle colloquialisms inherent in the language. However, the use of native speakers is not, ipso facto, a total solution to the problem. Only rarely is it possible to find one who can put the information down on paper in good English; his usual procedure is to transcribe what he hears into the Chinese characters of his native language, usually in the cursive script, which is a shorthand form referred to as "grass writing." But understanding this form requires a well-trained linguist -- [redacted]

NSA and the Service Cryptologic Agencies (SCA) rely upon the use of military men trained in spoken Chinese who interpret what they hear and put on paper, in English, their translation of what is transmitted. (In NSA these are erroneously called "transcriptions"). Intercept tapes that the military linguists are unable to translate must be sent to [redacted] NSA for translation. Seldom are field-translated "facts" called into question, and the only way that NSA can check their accuracy is to request the original tape from the intercept site -- if it has not been erased after the lapse of the 60 days permitted by current instructions. Few other SIGINT problems accept the risk of erroneous field translations so trustfully.

Few of these young military voice transcribers have worked with the language long enough to develop the vocabulary or experience to cope with colloquial words or phrases that go beyond the routine, stereotyped military language for which they have been trained. Furthermore, neither NSA nor the Service Cryptologic Agencies (SCA's) are likely to expend the time and money required to develop the large number of really expert linguists that are needed at intercept sites to translate (transcribe) voice intercept with the degree of accuracy that NSA's mission requires.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

How, then, can the present system be improved? The optimum is to have thoroughly seasoned linguists at the point of intercept; lacking this capability, the system must be geared to the capabilities of the personnel involved. As noted above, professional linguists at the point of intercept are not likely to be provided, so it may be necessary to consider a plan utilizing less qualified personnel and change to a new technique. By using PINYIN [redacted] as a time-saving shorthand device where possible, military linguist transcribers in the field could turn out true transcriptions that retain the original terminology for analysts to check -- if checking is really necessary.

PINYIN is the official CHICOM romanized spelling of sounds in the Chinese language. PINYIN was invented in 1957 for a variety of reasons, both practical and political.

Translation of the PINYIN [redacted] is the next problem to be considered. The transcribers could translate the material as they go (or later), either in the right-hand margin or directly beneath the Chinese PINYIN. In my opinion, written translations are not necessary until they become essential for the analyst or reporter's understanding of the transmission, or for inclusion in a SIGINT product report. Visual (mental) translation should be sufficient for most analysts familiar with stereotyped text - and it is not as difficult as one might think. In effect, traffic analysts reading Morse and teleprinter chatter [redacted] are (right now) doing just that -- reading Chinese (even if imperfectly). And if all analysts are thus forced to absorb some slight knowledge of the Chinese language in order to do their job (and do it better), wouldn't this be an additional benefit to the Agency? And who knows how many of these non-linguist analysts might develop into competent linguists after formal training in the language?

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

THE CREATIVE TRANSLATOR

by Tom Glenn, B61

"It is essential that the captain take steps to assure an attack as soon as possible," the translation read. "No delay will be accepted." I knew that the text in question has been passed in the heat of battle, by a man desperate in the face of imminent defeat and possibly death. It struck me that his language was rather formal for the occasion. The original read, "DAIJ UYS DANHS CHO DWOCJ CANGF SOWMS CANGF HAY LAF CHUR YEEUS CHAAMJ ZIF KHOONG DWOCJ." I would have translated it, "Strike soonest without fail. ((Time)) is of the essence. Any delay will mean failure." The first translation was not wrong, It simply missed the point.

The example is an extreme one (and it has been somewhat altered to protect the guilty), but it is symptomatic of a tendency of translators to smooth out the unruliness of the original, to impose order and business-like calm, to express everything in unruffled government English. When we do this, we destroy the vitality of the original, dehumanize it, and distort it. In so doing, we do our customers a distinct disservice to say nothing of insulting their maturity.

This article, then, is a plea for more creativity in translation. Unlike other disciplines where there is only one right answer, translation plunges the practitioner into the world of ambiguity where there are plenty of wrong answers and many right ones. The choice of the most nearly accurate answer depends not on dictionaries, grammars, and TECHINS, but on intelligence, emotion and understanding. For translation is rooted in language, which is first and foremost a sensual thing irretrievably tied to feelings in the chest, throat, mouth, nose and ears, and heavy with emotional cues. But language is also our primary means of information communication and bringing minds out of darkness. And as any linguistics student will tell you, language is erratic, syncretic, and dynamic. In coping with such an animal, creativity -- the ability to deal with the unknown and find new answers -- is simply necessary.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

There is nothing particularly revolutionary in any of the foregoing. But, surprisingly, we largely ignore the need for creativity in translating. Our rule-ridden procedures with programmed solutions for all eventualities are in part to blame. We have sought, as most organizations do, to take the the uncertainty out of our daily work by promulgating proper procedure appropriate to whatever circumstance. For translating it is a futile effort. For no matter what the girth of our guides, glossaries, grammars, dictionaries, memos, lexicons, manuals, and primers, we cannot replace inventiveness with rules. But since we have tried so valiantly to do so, we can hardly blame our translators for believing that modalite is always translated as "procedures," or that 利用 invariably means "exploit." What we have done, in effect, is make admirable progress in achieving machine translation from human beings.

Fortunately, it doesn't work. One reason is that words mean such different things to different people. As an Irish nurse once explained to me, "the screw" in the British Isles is slang for "wages." Similarly, "Defense de trepasser," as a sign on a cemetery gate in Canada announces means "no trespassing," not "no dying;" in the same part of the world, "chars usages" means "used cars," not "shopworn chariots." The influence of Americans on the nations of Southeast Asia has produced new hybrids. A sign in Saigon warns "Pas de fumer n'est permis" -- a French version via Vietnamese of the redundant military English, "No smoking allowed." In some oriental languages it is impolite to answer "no" to a superior. Thus, a Vietnamese who worked for me in Saigon, in trying to adapt to American casualness, answered most of my questions, "Da khong a" -- "Yes, no, sir." In English, "no doubt" often means there is some doubt; "fat chance" means "small likelihood;" and "Surely you don't mean that" means, "My God! You mean that!"

Despite these and other problems, translators persist in trying to program themselves. We could help them in three ways. First, we should emphasize mastery of English, a factor in translation we have overlooked with dogged consistency. First rate translation, after all, requires a profound understanding of the way English works, how it can be driven, shaped, cut, and tooled to make it catch the sense and feeling of the original.

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

Second, we should train translators -- and especially B Group translators -- to become comfortable enough in the foreign language that they can sever their dependence upon English to understand foreign texts. In essence, translators should be able to read a sentence in the target language, understand it without reference to English, and only then take up the question, "How do we say that in English?" Aids to reaching this stage are a good ear well tuned to the sound of the target language, a willingness to grasp at the basic meaning of a word which has no equivalent in English ("lai" in Vietnamese, for example, has only one meaning, not the half dozen dictionaries give), and ability to think without recourse to words. "Voila," can best be understood in terms of gesture and facial expression; "Khoi" in terms of picture of a circle and things outside it.

Third, we should encourage cross training of linguists, ideally in related languages. Chinese is the Latin of Southeast Asia; knowledge of Chinese is a valuable asset to Vietnamese, Korean, and Japanese linguists who must struggle with borrowed words often very difficult to translate. Thai and Lao are closely related. And so on.

Finally, and perhaps most important, translators must learn to unleash their minds. Rote translation works for some texts all of the time and all texts some of the time, but not for all texts all of the time. It is at this juncture that creativity -- the choice of right phrase or word in English to match the thought and flavor of the original -- becomes crucial.

\*\*\*\*

"A translator hath nede to lyve a clene lif, and be ful devote in preiers, and have not his wit occupied about wordli thingis, that the Holi spiryt, the autour of wisdom and kunnyng and truthe, dresse him in his werk and suffre him not for to erre."

.....Wyclif

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

ANALYZATION OF DATA

by Richard V. Curtin, B11

An analyst should first study data in its original form looking for obvious or significant points. By all standards it is most important that an analyst look for virtually any and all signs of unusual conditions which could occur in any form, in any data.

Customarily a thorough analysis is a primary goal but prior to any thorough analytic study, much can follow from initial scanning of data looking for virtually any important sign or signs. Do this first! From this point, particularly having run out of initial scanning of data, an analyst who works with traffic should dirty his hands by actually handling and sorting traffic in its original hard copy form.

Going through traffic, occasionally voluminous amounts of traffic, is a duty of all analysts. Having to do this has its applications to follow-on analysis. In this follow-on analysis many sound conclusions may solidify by improving facts first found during initialization. Just to avoid confusion, analysis is not sorting traffic -- it is a logical accounting for all individual parts of a main body of data.

Knowing functions and limits of said individual parts is important. Looking at all parts individually and as a group is also most important. Missing parts could focus on basic primary origins of data. Non-association of parts could add support to analysis also.

Odd or unusual conditions should aid in producing a working copy of an original body from which your data was forthcoming. Primarily, in addition to analysis of data, an analyst must list all significant facts for historical background information. Quick logical draw back of this information is an important point in analyzation. Random approach to draw back of data is not satisfactory in most situations.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Should various arts and skills apply, an analyst must vary his attack accordingly. This is a sign of a good analyst -- pliability or adaptability to situations and changing conditions. Until an analyst displays this quality in his analysis, an analyst is not functioning at a maximum standard.

Vital to all analysis is a thinking analyst, with ability to occupy his mind with various and sundry points. Which point to disavow or disclaim and which to follow-up is not always obvious. X-ray vision would aid any analyst, in both scanning of data and looking into goals of tomorrow.

You, as an analyst, occupy a vital position in an analytic community -- much of your analysis is original with no duplication by co-analysts, thus your analysis is primary to analytic community goals and missions. Z-groups and A-groups of valid data groups should aid cryptanalysts in locating indicator or discriminant groups and in turn aid in important cryptologic findings.

(Did you do any analysis of this data?)

(Editor's note: We will have further comment on this article in the December issue of Dragon Seeds.)

\*\*\*\*

PLAIN ENGLISH

One should hyperesthetically exercise macrography upon that situs which one will eventually tenant if one propels one's self into the troposphere.

Look before you leap.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

## CRYPTO-SCRAMBLE

*Richard Atkinson*

Unscramble each of the five numbered crypto-scrambles, placing one letter in each space, to form five words or names, each of which fits the definition to its right.

1. B I L L I T E A R

\_O\_ \_ \_ O\_ \_ \_ \_

Substitution method involving two cipher characters for one plain character.

2. T R I P E B A I T

\_O\_ \_ \_ \_ \_ O\_ \_

System in which the cipher units may be divided into two separate parts, each with clearly defined functions.

3. A G R I D C H I P

O\_ \_ \_ \_ \_ \_ \_ \_ \_

Substitution method in which the plaintext units are treated as pairs of characters.

4. V A I N S T A R

O\_ \_ \_ O\_ \_ \_ \_

Two or more cipher symbols which have the same plain equivalent.

5. A N A I D

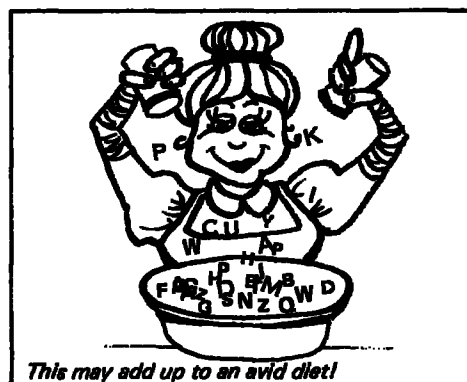
O\_ \_ \_ \_ \_

RYE program which produces digraphic distribution and statistics.

Now arrange the circled letters to form the cryptoanswer suggested by the cartoon at the right.

Print CRYPTOANSWER here

\_\_\_\_\_

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~SEEDLINGS

----The 10th Professional Qualification Examination in Cryptanalysis will be given on Monday and Tuesday, 15 and 16 November 1971. Personnel who wish to take any or all parts of the examination should contact the CACP office, Room 3A116, 3868s by 5 November 1971. Anyone interested in attending prep sessions for the examination should contact Al Verbitz, B03, on 5296s.

\*\*\*\*

----PQE #5 will be administered by the Traffic Analysis Career Panel in the north side of the NSA FM cafeteria on Monday, Tuesday and Wednesday, 6, 7, and 8 December 1971. A new TACP study outline has been prepared for distribution to all aspirants. To ascertain eligibility, candidates should submit PQR's, addenda, and reports to the TACP office, Room 1C190, by 5 November 1971.

\*\*\*\*

----The Language Career Panel is investigating the possibility of requiring all candidates for certification to demonstrate their ability to understand their target language as spoken formally. The requirement would not be rigidly imposed for several years (1975 is being mentioned) to allow for the arrangement of proper training.

\*\*\*\*

----"The SEATS Message Log - Building a Cryptanalytic Tool," published by B65 is an excellent summary of the current SEATS processing cycle. Although written for cryptanalysts, traffic analysts who'd like to understand more of the processing behind-the-scenes can learn from this well-written report. It's B65-SSR-02-71 dated 15 August published by B654.

\*\*\*\*

----A compilation of various briefings given during the February 1970 "Traffic Analysis Mechanization Forum" was published recently. Twenty-four briefings were delivered at the

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

forum including four B Group presentations: "Introduction to T/A Mechanization," R.S. Benjamin; "Southeast Asia" by Fred Mason and Dick Alexander, and "Vineland" by Dick Wilschke. Copies may be obtained from Mrs. Gloria Chiles, P14, 5868s.

\*\*\*\*

----Virginia Jenkins, E13, who is developing the new course, "Practical Diagnosis" - CA 260, which deals with the cryptanalysis of hand systems and cipher devices and features operational problems, is soliciting input from B Group. Of particular interest are cipher systems employing non-cyclic additives, and rail-fence or grill transposition.

The pilot class in CA-260 was held between 15 March and 17 May 1971. The next class is scheduled for March 1972. Persons interested in attending or who have subjects for inclusion may contact Virginia Jenkins on 8-8016s.

\*\*\*\*

----The Council of Learned Organizations (CLO) is planning a symposium to acquaint the NSA community with the interrelationships that exist among the major cryptologic disciplines, with computer serving as a unifying theme, by means of lectures, exhibits and tours. The event is scheduled to take place in March 1972.

\*\*\*\*

----In an effort to cultivate professional linguistic activity throughout the cryptologic community, the Crypto-Linguistic Association is encouraging the formation of Special Interest Groups. For particulars, contact Dr. Amelia Murdoch, 4767s.

\*\*\*\*

Articles for publication may be submitted through Division Press Corps members or directly to DRAGON SEEDS, B03.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



EO 3.3b(3)  
PL 86-36/50 USC 3605

ASK  
THE  
DRAGON  
LADY

Dear Dragon Lady:

In planning the itinerary for [redacted] forthcoming visit to PEKING, please try to arrange an opportunity for him to visit the Gate of Heavenly Peace in the old city of PEKIN [redacted]

If the time can be found, he should also visit PEIP'ING, [redacted] particularly for a view of the T' IEN AN MEN and its striking architecture.

During the period of his visit he might be able to arrange a side trip to both PEICHING and BEIJING enroute to or from the airport.

During the [redacted] stop at CANTON a short sightseeing trip around KUANGCHOU and GUANGZHOU should also prove interesting.

LAWRENCE ST. CLAIR MYERS  
B441, 4637s

\*\*\*\*

The Dragon Lady received the following two letters referring to problems of terminology, so she passed them on for authoritative comment to our A-number-one glossarist, the Guru and Caudillo of the Dundee Society, Lambros Callimahos.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Dear Dragon Lady:

What is high-grade traffic?

Is it that type which is machine enciphered? If so, why do areas with no machine enciphered traffic categorize some of their traffic as such? Is it the type in which an additive is applied to an already enciphered text? What if the generation method of the additive stream is exploitable? Is it user-related?

These are just a few of the ambiguities I have encountered. The BASIC CRYPTOLOGIC GLOSSARY, June 1965, defines high-grade as "Of a cryptosystem, offering relatively great resistance to cryptanalysis." How does one measure "relatively great resistance?" Is it in the eye of the beholder? If so, then all of the above truly be high-grade.

Can you offer a more precise meaning for this oft used term?

CAROLYN Y. BROWN  
B1122

Dear Carolyn:

In answer to your question, let us examine for a moment three definitions as found in the first (1955) edition of the Basic Cryptologic Glossary:

"low-grade, adj. Pertaining to a cryptosystem which offers only slight resistance; for example: (1) Playfair ciphers, (2) single transposition, (3) unenciphered one-part codes."

"medium-grade, adj. Pertaining to a cryptosystem which offers considerable resistance to cryptanalysis; for example: (1) strip ciphers, (2) double transposition, (3) unenciphered two-part codes."

"high-grade, adj. Pertaining to a cryptosystem which offers a maximum resistance to cryptanalysis; for example: (1) complex cipher machines, (2) one-time systems, (3) two-part codes enciphered with an additive."

These definitions were dropped from the second (1965) edition,

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

because obviously the relative security of a cryptosystem is in the eye of the beholder: a single transposition cipher may well be a high-grade system (as for example a certain German World War II cipher); and a "one-time" system may be low grade if the Fibonacci generating-group, even if randomly chosen, is sent in the clear as the A1 group of the message. A two-part code enciphered with an additive book may be a high-grade system if the code book is unknown, the additive book large, the indicator groups enciphered, and the cryptoperiod changed frequently; but if the code book is known, the additive book small, the indicators sent in the clear, and the keys in effect for a long period, the system would probably qualify as a low-grade system. All of the foregoing remarks apply to our cryptanalysts; a cryptanalyst from an emerging African republic might find it impossible to cope with a Playfair cipher, and so as far as he was concerned it would be a high-grade system. And so, Carolyn, the definitions for low-, medium-, and high-grade cannot be made more specific, since they are so subjective.



\*\*\*\*

Dear Dragon Lady:

I am a newcomer to the world of manual cryptosystems and the jargon has me completely confused. There is a definite terminology gap between "the honorable elders" and the neophytes like myself who have just completed basic CA courses. In fact, there even seems to be a terminology gap between the different training courses (i.e., CA-100, CA-400, CY-100).

For example, what is biliteral substitution? The 1965 edition of the Basic Cryptologic Glossary defines it as "encipherment by substitution methods in which the cipher text units are pairs of characters." What about the plaintext units? If the size of the plaintext unit is larger than one element (medial plus final or medial plus final plus tone) is it not now digraphic? Suppose variants are employed on a digraphic system (where plaintext unit size is larger than one) is the system digraphic with variants, code chart with variants, or is it all lumped under biliteral with variants?

~~TOP SECRET UMBRA~~

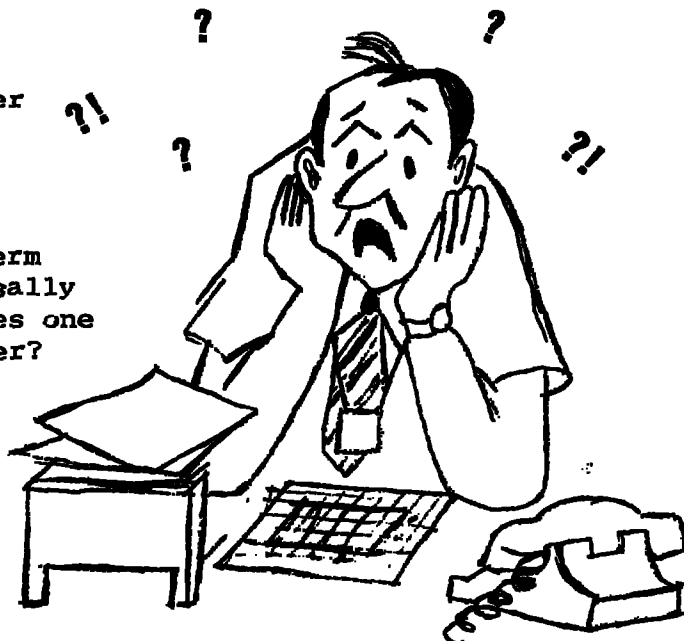
~~TOP SECRET UMBRA~~

Is a dinomic system included under biliteral or digraphic .... or both?

And finally, why has the term "unilateral" replaced the term "monoalphabetic" which is universally recognized and accepted? How does one refer to the basic units of cipher? "Unilits?" "Bilits?" Where is the new crypt glossary?

HELP!!

DAVID J. SHEPARD  
H11



Dear David:

First of all, David, you must realize that some "honorable elders" are just older, but not necessarily wiser: we have some first-class technicians who would flunk freshman English. Again, the terminology gap between different training courses is a function of the glossarial erudition of the particular instructor. Now for your compound question.

In biliteral substitution the cipher elements are pairs of characters, regardless of the size of the plaintext elements (which may be single letters, pairs of letters, or even units of larger size); in digraphic substitution the plaintext elements are indivisible pairs of characters, regardless of the size of the cipher elements (which may be, for example, pairs of letters, trinomes, or other combinations). A Playfair cipher is digraphic (because the plaintext elements are indivisible pairs of letters), biliteral (because the cipher elements are pairs of letters), and monoalphabetic (because there is a one-to-one correspondence between plain and cipher equivalents)--although the latter should not be stressed lest it confus young, impressionable minds or incense older, stultified ones.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

A "digraphic system with variants" is self-explanatory, as is "code chart with variants" if a code chart were involved; "biliteral system with variants" would usually imply variant coordinates in connection with some kind of a cipher square. A "dinomic system" is either a biliteral system, or one in which plaintext dinomes are subjected to further cryptographic treatment.

A simple substitution cipher is monographic (because the plaintext elements are single letters), uniliteral (because the cipher units are single letters), and monoalphabetic (for reason given above). Cipher elements are called "characters," "digraphs," "trigraphs," etc. The third (1971) edition of the Basic Cryptologic Glossary, which has just been completely revised, should be printed and distributed during November.

Any further questions?



\*\*\*\*

"It is only when there is some mortal deserving of being delivered that the single live hair of the most excellent Buddh protrudes itself and stands forth in a straight line from between the eyebrows."

---the Manual of Buddhism

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

## CONTRIBUTORS

PEGGY BARNHILL, a data systems analyst in B42, is a 1966 graduate of Marywood College, Scranton, Pa. She completed the SR Intern program in 1970 and is currently working on the software specifications for the AG-22 processing system within B Group.

DICK CURTIN, Deputy Chief, B11, entered on duty with NSA in 1950. After initially working on the Soviet problem, he was selected for the first class of CV-100 and subsequently became involved in cryptanalytic attack on various A, B, and G problems. He received an NSA scholarship to complete his bachelor's degree in mathematical statistics from the George Washington University. Mr. Curtin is certified by the CA, TA, Data Systems, and Mathematics Career Panels.

AL GILBERT, B6403, came to NSA in 1966 after retiring from the Army Security Agency as a CW3. While in ASA, he served in Europe, the Far East, SE Asia, and at NSA, working at various times as reporter, traffic analyst, Russian linguist and cryptanalyst. Mr. Gilbert, who is professionalized as a Special Research Analyst, has worked on the Vietnamese Communist military problem since 1966.

TOM GLENN, Deputy Chief, B61, has a total of thirteen years experience with ASA and NSA on the Vietnamese problem. He is a professionalized special research analyst and Vietnamese linguist who has also studied Chinese and French on his own. Mr. Glenn has served as the chairman of the Vietnamese Language Professionalization Examination Committee. Assigned to Vietnam in 1962-1965, 1967-1968 and 1969, he has been involved in traffic analysis, cryptolinguistics, intelligence analysis, and - most significantly - in the management of the SIGINT reporting effort on the Vietnam war.

DONALD LENAHAN, a cryptanalyst in B22 on the CHICOM [redacted] problem, entered on duty with NSA in 1967. He completed the CA intern program with assignments in A, B and G Groups, and is professionalized as a cryptanalyst. He holds a B.S. in German from Manhattan College and is working on a master's degree at Georgetown University.

EO 3.3b(3)  
PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

L. ST. CLAIR MYERS, CHICOM bookbreaker and [redacted] Coordinator in B44, is also a qualified bookbreaker and cryptolinguist in Russian and Japanese. During his U.S. Navy service (1941-1966) he rose to the rank of Commander and served as Chief of the CHICOM [redacted], Officer-in-Charge of various NSG activities, and Chief of [redacted] and NSAPACREP Korea.

WAYNE E. STOFFEL, B03, began his cryptologic experience in 1946 with a three-year tour in the Army Security Agency. At NSA he worked on the Soviet problem until 1954 and on Asian targets thereafter. Mr. Stoffel was a member of the TA Career Panel from 1965 to 1971 and has been an associate editor of COMMAND since 1968. He holds a B.S. degree in physics from Johns Hopkins University and is certified in the TA, CA, SRA, and Physical Science Career Fields.

CHARLES SWIFT, B6404, served four years in the Air Force Security Service as a traffic analyst on CHICOM [redacted] and on the Vietnamese Communist problem during the pioneer stages of SEATS. Following his conversion to civilian employment at NSA in 1966, he has worked in the Vietnamese Communist support division, and has recently been reassigned to B61.

PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~

Do

*Remember !*



*It's classified*

~~TOP SECRET~~

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

MAR 72

PI  
Mr. L. D. Callimahos

~~TOP SECRET~~

# National Security Agency

Fort George G. Meade, Maryland



THIS DOCUMENT CONTAINS CODEWORD MATERIAL

~~TOP SECRET~~



~~TOP SECRET UMBRA~~

This is Dragon Seeds.

There is fantasy, irony, and the bite of reality in the name. It speaks of the East. And, like the East, it suggests much, says little.

Dragon Seeds is both Mother China and her neighbors. Dragon Seeds is monumental and minuscule. It is the past and future. It begs for elaboration but gives none. In it are echoed softly slurred Mandarin, brittle Vietnamese, determined Korean. In it is the spectre looming over the Thai, Lao, and Khmer. It is frightening and friendly. It is uncertain.

Above all, Dragon Seeds is promise. It is fertile with ideas unbounded, to be cultivated with creativity and imagination. It is challenge. It is alive. It will be more than it is.

Dragon Seeds is yours. May it grow with you.

The Editors

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

DRAGON SEEDS

Publisher

DONALD E. MC COWN, CHIEF B03

Managing Editor

Minnie M. Kenny

Executive Editor

Robert S. Benjamin

Composition

Helen Ferrone  
Lorna Selby

Copy Editor

Thomas L. Glenn

Rewrite Editor

Victor Tanner

Special Interest Editor

Ray F. Lynch

Biographical Editor

Jane Dunne

Education Editor

Marian L. Reed

Feature Editor

Richard V. Curtin

PRESS CORPS

B11 Carolyn Y. Brown

B12 Philip J. Gallagher

B21 Gary Stone

B31 Jack Spencer

Thomas M. Beall

B32 Jean Gilligan

B33 Louis Ambrosia

B34 Thomas L. Wood

B41 James W. Schmidt

B42 Velma Jefferson

B43 Mary Ann Laslo

B44 Jack L. Thomas

B45 John E. Uzarek

B5 Paul M. Hoagberg

B61 Ted Lukacs

B62

B63 Jean C. Smith

B64 Allen L. Gilbert

B65 William Eley

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605Vol. 1  
Nr. 2

March 1972

## TABLE OF CONTENTS

Mr. Kern's Salutation		1
Reflections on Cryptanalytic Accountability	George Patterson	2
CHICOM Development <input type="checkbox"/> and the AG-22	Philip Remsberg	7
MFMUFS and Catnip	Michael Nugent	12
The Open Door: CAMINO	Mary D'Imperio	15
The Importance of Being Honest	Al Gilbert	20
China-Wide Technical Specialists: A Way to Save Overseas	Stanley Waddell	21
The Strategic Importance of Shenyang Military Region	Claire Smith	23
How Great COMINT Facts from Little Slivers Grow, or Making Russian Molehills Out of Chinese Mountains	John Mollick	26
Seedlings		30
Ask the Dragon Lady		33
Contributors		40

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

It is with great pleasure that I add a few remarks to this, the second issue of *Dragon Seeds*. The success of the first issue warrants an expectation of exciting issues to come and this somewhat delayed second issue gives substance to that expectation.

The first issue of our informal house organ opened a few gaps in the psychological walls between linguist and machine man, cryptanalyst and reporter, technician and manager, trainee and professional. It did more; it crossed barriers between targets to show one area what another was doing or hoped to do and perhaps to stimulate investigation into using someone else's procedures to do our jobs. If succeeding issues meet the standard of the first, we will have a communication vehicle of unquestionable value to all of us in B, regardless of our individual specialties.

To mention some of the benefits that I will derive, *Dragon Seeds* can give me insight into aspects of daily B Group operations -- rewarding or frustrating -- which I normally do not have the opportunity to view. Through its articles and columns I look not only to rejoice with analysts whose own technical projects have begun to pay off but also to explore new paths with those who ask, "Why can't we...?" or who propose "We can accomplish..."

I congratulate all whose interests, skills, and actions have brought *Dragon Seeds* to life. A special "well done" to the Dragon Lady.

*Richard W. Kern*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605A REFLECTION ON CRYPTANALYTIC ACCOUNTABILITY AND EFFORTS  
by George Patterson, B65

This paper contains some of the thoughts and conclusions reached by this cryptanalyst during the insidious search for pertinent homogenous cryptomaterial being transmitted on some of the Vietnamese Communist Morse nets using one-time pad cryptosystems. If, at times, it reflects an attitude of despair, please remember that this is an honest effort of accountability being offered with the hope of modifying future efforts and hopefully producing usable product. My periods of despair were never caused by the ability of target echelons to transmit secure communications [REDACTED]

On a brighter note, the picture is not altogether as bleak as the phrase "one-time pad exploitation" implants in the minds of most people. Some change is already underway in my organization to make the cryptanalytic approach to the homogeneity problem less awesome and irrevocable than originally viewed by this author. So please permit me to present my position and some reflections and observations that led me to write about them.

Impressions and Ruminations

My first thought is of a non-technical nature. It is my opinion that those who pronounce one-time pad exploitation as being near impossible are simply anchoring their conclusion in the sea of unread one-time pad enciphered messages. This brand of truth-telling often reflects the self-delusion that says "If I can't do it, neither can you." When this attitude influences policy decisions to the point that exploitation is unnecessarily difficult, then we are where I believe we are today. Does the interest justify the revaluation of existing practices?

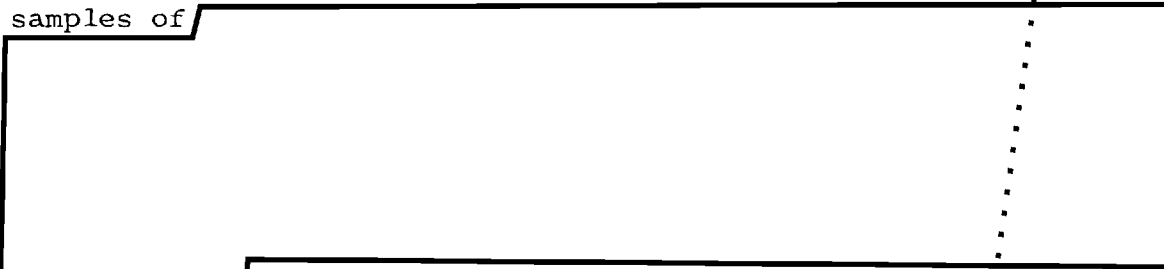
My second thought is a question. What are we looking for in researching one-time pad systems and can we explain our interest in objective measurable terms? The answer is twofold and I believe that here is where we enter the first area of confusion insofar as policy decisions are concerned. Cryptanalytic research is research and very often not accountable in the form of estab-

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

lished criteria or results-oriented job performance requirements. Cryptanalytic housekeeping on the other hand is, or at least should be, an integral part in the development and maintenance of the technical base from which the intelligence fact is derived.

A more technical explanation of each endeavor will be served with examples from my experience. A few years ago I took samples of



What was I trying to do? I was simply applying cryptanalytic techniques to one-time pad systems users and I produced product. So when someone said "Have you ever read a message Ha Ha;" I simply viewed that someone with benevolent amusement because I had my network diagram to keep me warm. The research of the Pathet Lao network continued because the ideal situation for limited code recovery existed. That is, a network with each terminal transmitting on a single cryptolane sending sequential messages while utilizing one code which was enciphered sequentially through one [redacted] at a time.

When a cryptanalyst is researching, he or she is not unappreciable of good raw material that is available and this includes the uncomplicated number serialization and sequential key pad usage by the target crypto-center. I was probably more appreciative of uncomplicated serialization because as an ex-Morse operator I knew that theoretically a station may transmit a message that is followed by a message that serves a different originator, a different recipient, has been encoded from a different key source, utilizing a different transmitting system and yet be sent out on the same schedule. Schedules, callsigns, frequencies and times of transmission do not necessarily denote that the messages being sent on a given schedule will be cryptanalytically homogenous in any way. Comm-center serialization necessities, relay priorities and the transmission of more than one system on a given schedule are just some of the problems that can be encountered. Yes, homogeneity can hit the proverbial fan.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

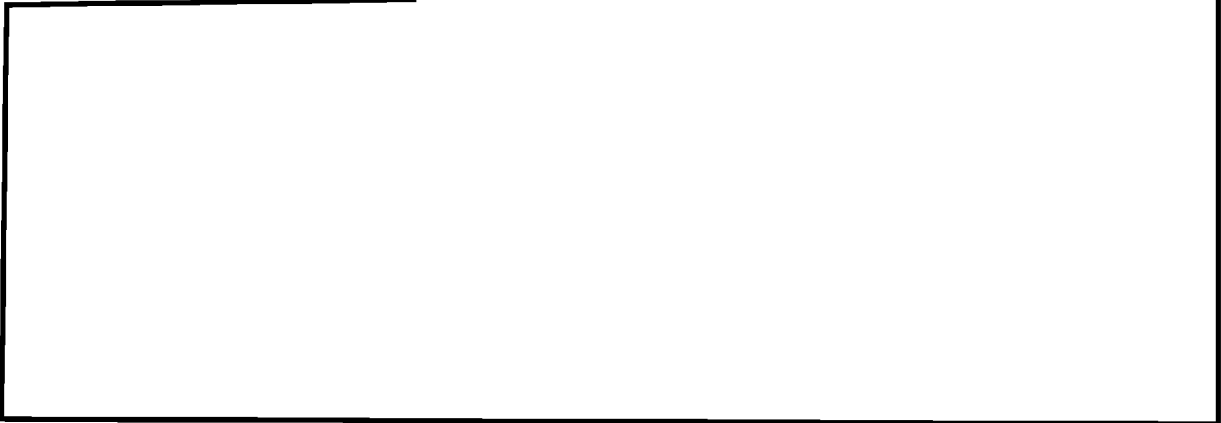
Research of cryptographic practices on the Pathet Lao nets was possible because good cryptanalytic housekeeping was possible. Note that I am not confusing good traffic analysis with good cryptanalytic housekeeping. They are not one and the same. A given schedule may announce the communication between stations or it may be a broadcast. How the material sent will fit into the crypt-household is a task for the involved cryptanalyst.

The point to be made is that the successful extraction of homogenous crypt-material is directly proportional to the operating procedures that are forced on target entities. The Laotian communicating procedures are much more orderly than those for the Vietnamese Communist military. The honeymoon was over when I began doing research on the Vietnamese five-digit one-time pad systems.

The Vietnamese Situation

It appears that the main hope of compiling homogenous material (on Vietnamese Communist [redacted] practices of the target. In other words, I believe that the cryptanalyst must look to the communications center for his salvation. [redacted] should present a better over-all picture of the crypto-practices of each entity.

For instance, the posting of a schedule originated from the Vietnamese Communist [redacted]



~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~



In this case traffic analysis pinpointed the active cases with the usual where and when accuracy. The crypto-practices of the radiostations involved made the extraction of homogenous material extremely complicated. Many reasons for such situations come to mind. One obvious reason is the existence of more priority messages in a military situation. They can reflect themselves in the form of what appears to be mixed-up sequence. When several high precedence messages are received in the message center and numbered along with low precedence messages the result is the high precedence messages will be sent out along with an earlier sequence.

Although the traffic analyst provides the when and where, the who and what are the needed tools of the cryptanalyst. These tools are needed on a delivery schedule that is realistic to the cause of cryptanalytic research. I have waited a large percentage of my four and a half years as a one-time pad analyst for machine sorts. Certainly this waiting period has forced me to be of less value to anyone seeking up-to-date crypt-knowledge. Since no person likes to be held accountable for variables over which he has no control a cryptanalyst must live with mixed emotions. He or she is often embarrassed while in conference with the traffic analyst because the traffic analyst is interested in current activity. By the time a cryptanalyst can measure the results that his enterprise yields it is sometimes "old hat." But is this not fully accepted throughout the cryptologic community as one of the crosses the cryptanalyst must bear?

What is the ultimate test of professional accountability? If the answer is proof of performance and if complexity and difficulty are not justification for ignoring the need for change, then I offer the following suggestions.

I suggest the need for a periodic assembly of persons involved with the investigation of a given echelon and its subsequent network of communications, the purpose being a realistic exchange of knowledge along with a results-oriented discussion of future efforts.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

I'm asking that cryptanalytic housekeeping begin with the message centers and that cryptanalysts be tasked with the responsibility of compiling homogenous material originating from a crypto-center regardless of the kind or number of systems being utilized by that center. This will provide, in handy form, the [redacted] search would be much easier. T/A assistance could be given with more confidence. Communications changes could be followed with more accuracy. System extraction from properly posted crypto-center [redacted] could be done with more ease and accuracy. Such a system would, most of all, allow us to introduce accountability into our crypto-practices. Fortunately, my ideas and suggestions were listened to and their merits weighed.

Postscript

Ironically, even as my point of view was being presented in this paper, a situation arose which provided the opportunity for applying some of the procedures that I have discussed. A [redacted] which were used by a recipient to decrypt and decipher [redacted]

[redacted] has provided me with the opportunity to apply my selfish methods of traffic sorting. [redacted] transmissions have been put in date order with total disregard to case notations, station NR serialization and systems. Messages are being sorted on a [redacted]

[redacted] Is it a crypto-center serialization? Is it an originator's serialization? Is it unique in its function? Do we really know? I do know that each [redacted] is restricted to the use of [redacted] and we have continuity. The [redacted] at a rapid rate and we have [redacted] The [redacted] is being enciphered at a much slower rate. The recipient was receiving messages in at least two different systems.

The willingness to change work practices that do not produce product and create practices that do, sounds good. Progress is a nice word, but change, its instigator, is not. It implies criticism. It shouldn't, since target crypto-practices are the reason for the need.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605CHICOM DEVELOPMENT [ ] AND THE AG-22  
by Philip Remsberg

How do the AG-22 and the machine programs designed to process its output affect the handling of CHICOM Development [ ] intercept? The article titled "The AG-22 and You," by Peggy Barnhill, in the first issue of DRAGON SEEDS describes the basic functions and the on-going programs which operate on intercept recorded on paper tape output from the AG-22 equipment. This article delineates a practical application of AG-22 processing by following an item of [ ] intercept through the AG-22 process from initial detection to identification or ultimate disposition.

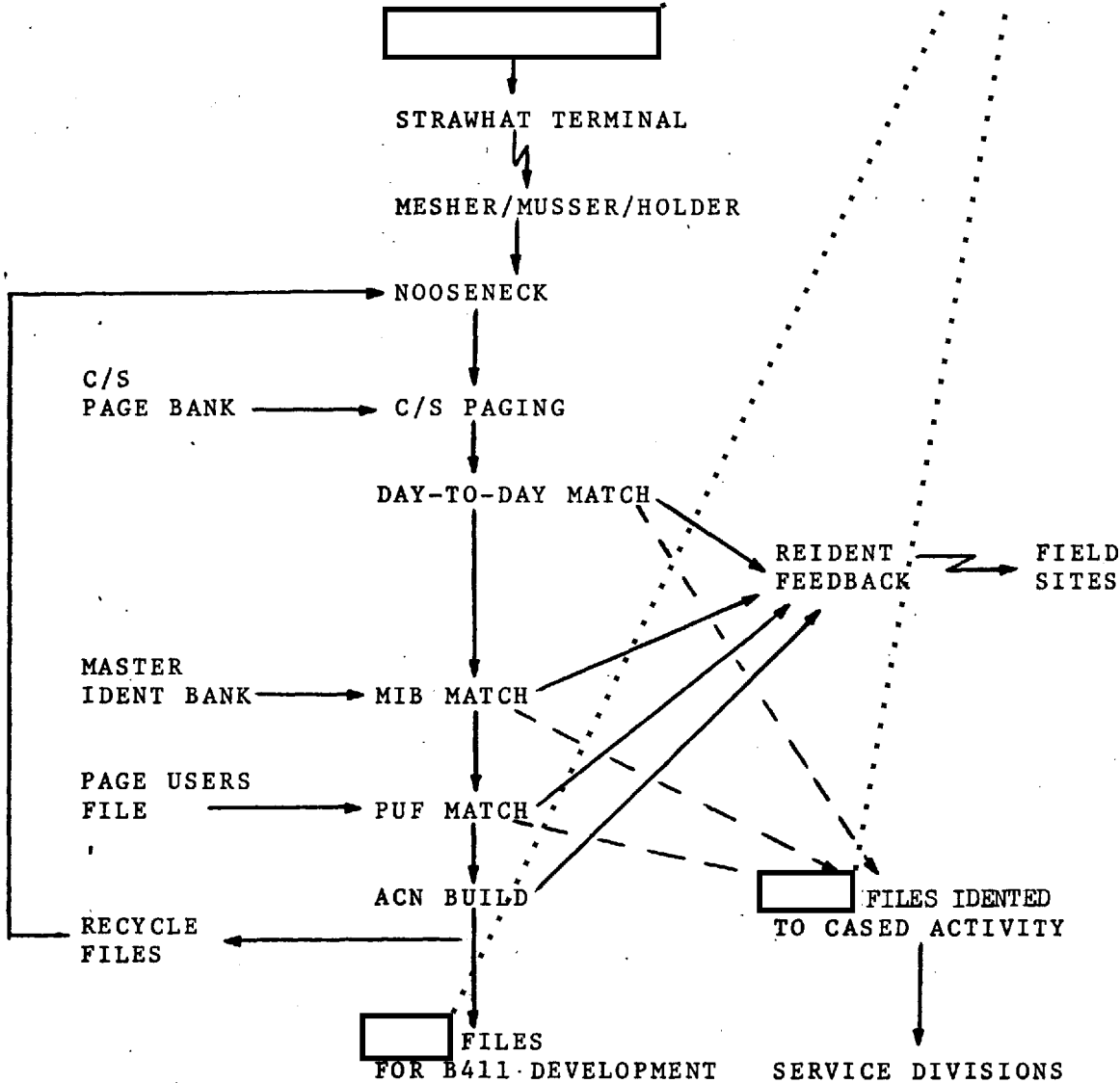
The intercept operator has a frequency spectrum assigned for search during periods when assigned targets are inactive. Activity detected during the search is to be copied for up to 15 minutes and attempts at identification are to be made. This search program is called HOMESPUN. Because the intercept operator does not have time for exhaustive attempts at identification, activity detected during search is most often cased [ ] conversationally referred to as a [ ] ditter. HOMESPUN raw traffic comprises approximately [ ] of the developmental material; the CHICOM Development Branch (B411) attempts to identify this material or maintains continuity until identification can be made. B411 has found that one of every three files can be identified to a known case notation. (A file is one intercept item of continuous activity from time-up to time-down which normally equates to one sked.) Identification of the large volume of files received daily would require a most cumbersome manual examination of callsigns. This task can be much more efficiently accomplished by the [ ] identification programs devised for use with the AG-22 input.

To illustrate, let us assume that, at 1509 Okinawa time, [ ] activity assigned to an intercept position at [ ] is inactive and that under HOMESPUN the intercept operator is copying a [ ] ditter. While the man is typing a hard copy, the AG-22 is spewing out an 8-level punched paper tape. The paper tape, which contains other files as well as our [ ] ditter, is soon picked up and delivered to the local terminal of the STRAWHAT data link for transmission to Ft. Meade. At the

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

FLOW DIAGRAM FOR [ ] DITTER THROUGH  
THE AG-22 PROCESS



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

NSA STRAWHAT receiving terminal, the data is recorded on a magnetic tape (MESHER/MUSSER/HOLDER) along with other [ ] ditters as well as cased files from other far eastern sites. About 2300 NSA time, the magnetic tape is mounted on a 360/85 tape drive, and the data begins its progress through a collection of programs known as the NOOSENECK system.

The first step in the NOOSENECK reidentification process is the paging of callsigns. All callsigns are compared against those in the A-02 and C-05 callsign page banks. If the transmitted callsigns appear in the page banks, page information is automatically recorded in the file. As the file continues through NOOSENECK, the callsigns and accompanying page information will be referred to many times.

The first attempt to identify the [ ] ditter by machine follows the callsign paging routine. The [ ] ditter under consideration was copied at [ ]. The same activity, however was copied at other far eastern sites and identified. Assume that USM-48 had identified the activity as [ ]. Except for possible garbles, the callsigns for both intercepts should be the same. A routine of NOOSENECK compares the callsigns of the [ ] ditter with all the callsigns of all the cased files that were received from all far eastern sites. An automatic identification is made when the 2-50 is satisfied. The 2-50 rule states that at least 2 callsigns and no less than 50% of the callsigns of any two activities being compared must match. For example, if five callsigns are being compared, at least three must match; if two callsigns are being compared, both must match. If a match is made, the [ ] ditter is labeled with the good case notation and with a distribution code so that at the end of the AG-22 process the file will be forwarded to the appropriate B21 analyst. Most [ ] ditter identifications occur during this day-to-day match, so called because it compares all callsigns in the files on any given day.

If the day-to-day match fails, the [ ] ditter enters the next NOOSENECK routine which compares the callsigns with those in the Master Identification Bank (MIB). The MIB contains all CHICOM callsigns observed during the preceding 5-day period as well as fixed callsigns of CHICOM [ ] and other activities along with associated case notations. Callsign matches must meet the 2-50 rule for an acceptable identification. Comparison

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

with the callsigns in MIB increases the chances of an identification in the event that the ditter matches a known activity which was not copied on the same day. Should a match be made, the identified item is labeled for distribution to the appropriate analyst.

Another opportunity for identification of a still unidentified ditter exists in the Page User File (PUF) program. The PUF contains the latest equations of case notations to callsign pages and constitutes a reliable, though not infallible, identification aid. PUF matching is based on page data which was collected during the paging process rather than on the callsigns, themselves, of identified activities. The 2-50 rule still applies but in relationship to the number of callsigns on a page; i.e., at least 2 callsigns or 50% of the callsigns used by an activity must be on the same page. If the rule criteria are met, the PUF is checked to ascertain whether a particular case notation involves callsigns selected from that page. A positive finding results in the appropriate case notation being placed on the ditter; a negative finding results in the generation of a page Arbitrary Case Notation (ACN). A page ACN is automatically assigned by machine when callsign usage meets the 2-50 rule for a callsign page but no case notation equation for that page exists in PUF.

Activities that remain ditters may eventually be assigned a 2-day continuity ACN or otherwise identified by the day-to-day or MIB match because ditters remain in the file for 5 days. Callsigns are compared each day and when the same callsign has been observed on 2 different days, a 2-day continuity ACN is automatically assigned. These ACN's eventually find their way to a 2-day continuity analyst who attempts identification by other means or retains them for further development.

When intercept is identified to a known activity, selected data is provided to the field station tasked with that particular activity within 24 hours of the original intercept. This data which includes case notation, date of intercept, frequency, and time up, enables the field station to take advantage of unique intercept whether copied at that station or picked up during search at another. Technical data for intercept that has been

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~

assigned an ACN is also provided to the intercept station within 24 hours to help follow-up copy of the activity. Any follow-up copy will assist the analyst in making an identification or in maintaining continuity.

CONCLUSION

The AG-22 and associated machine programs will enhance analysis of CHICOM Development [ ] intercept. More timely analysis is possible because full copy of intercept for the preceding day can be placed on the analyst's desk each morning. Matching processes have pulled together all related [ ] intercept, and [ ] continuities are readily discernible by machine-assigned ACN's.

Any [ ] intercept that can be identified to a particular CHICOM service entity is properly labeled and forwarded to the appropriate analytic section. Thus, all intercept for any given day is available at once even though some may have arrived at NSA as unidentified.

The AG-22 process now serves traffic analysts well. We can surely look forward to new programs that will do even more for the analysts and for the CHICOM problem.

ไฟล์ โป้เพ็ง

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

HFMUFS AND CATNIP

by Michael J. Nugent, B45

Aids to B45 Traffic Analysis and Collection Management

For several years the Agency has been working on techniques for describing the environmental factors or conditions that affect the propagation and intercept of radio signals. The object was to develop a capability for readily determining our chances of intercepting a given signal at a given time at a particular intercept site. As a result NSA now has accepted reliable computer programs which contain mathematical models of electromagnetic radio wave propagation conditions.

The High Frequency Maximum Usable Frequency Systems (HFMUFS) program was developed primarily to aid the telecommunications engineer and manager in planning for worldwide U.S. radio circuits in the 2 to 30 MHz range. This program has been applied to many facets of the SIGINT problem. Some of these include analysis of target country communications circuits, analysis of SIGINT site antenna configurations, and skywave support as an aid to collection managers for tasking against targets working up to about 50 MHz.

The Computer Analysis Target Network Intercept Potential (CATNIP) program employs essential routines from HFMUFS for determining ionospheric parameters. CATNIP considers three factors: transmitter, intended receiver, and intercept site. Basically, the program performs statistical studies of the characteristics of a communication link to determine the probability of ionospheric support and the probability that the target transmitters will generate enough power to make it interceptable from a specific point. This information is then used to determine the probability of intercepting the target emissions. These probabilities are computed as functions of month, hour, location, sunspot number, frequency, modulation, bandwidth, antenna, off-main beam-radiation, vertical angle of signal arrival, and environmental noise (including level of man-made noise). Target circuit data can be inserted into the program from punched cards or from magnetic tapes containing automatically reformatted TEXTA, the Russian Master Reference Library (RUMRL) or ICAL data files. The

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

program is used mainly to perform large studies for establishing guidance for redeployments of collection resources, contingencies, proposed new sites and to determine intercept capability at existing sites. CATNIP requires a minimum amount of target network input data and, based on this input, can generate additional data concerning the target links if required.

We in B45 were interested in the HFMUFS and CATNIP programs to aid us in determining the most probable geographic areas of reception for CHICOM [redacted]. These areas of reception are determined by inputting information on the location of the control, monthly transmitting schedule, frequencies previously observed, mode of communication, type of transmitting antenna and transmitting power. If diagnostic information were available on the type(s) of transceivers used by the outstation, it could also be input into the programs to determine the frequency and schedule limits these criteria impose on control and outstation communications. It should be pointed out, however, that all of the CHICOM [redacted] communications are transmitted as broadcasts. There is yet no evidence of any [redacted] outstation activity. Additionally, the type of control antenna and transmitting power are assumed so that the program results on outstation locations must be considered as suspect and used at this time only as reference points until some collaborating information can be obtained which would confirm or refute the results.

Because of the reduction in collection resources during these times of austerity, our target communications must be scrutinized more closely than ever to determine the maximum and most efficient utilization of cover. The CATNIP program, when supplied with previous schedule activity, control/outstation locations, antennas, and transmitting power, can analyze this information along with ionospheric changes which occur from month to month and determine the best collection site(s) to intercept a target's communications. These programs were successfully employed on the CHICOM [redacted] communications targets when hearability problems, resulting from seasonal changes, occurred (See "LVHP Propagation and Collection Techniques," by Raymond B. Harrison, in NSA Technical Journal, Vol XVI, Fall 1971).

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

Many variables are involved in the process of deriving intercept predictions. The more specifics that are known about the target, the more confidence can be placed in the results. However, even though only target locations, frequencies and modulation are known, a comprehensive analysis of the target environment and its relative intercept potential can be performed.

Some of the CATNIP routines previously described are only those which have been applied to the [redacted] CHICOM and Soviet [redacted] problems. A more in-depth and technical explanation of the CATNIP program, its options and applications, is contained in "CATNIP," by Robert B. Riegel, in the NSA Technical Journal, Vol. XVI, Winter 1971.

\* \* \*

"When I first came to the Agency, there were two persons I stood in awe of -- God and the Checker. As time went on, I really learned to fear that Checker."

Harry Rashbaum, B6

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~**THE OPEN DOOR**

*We seek to be companions along the way.  
 The lantern which we carry is not ours.  
 The spirit which we share is contagious thought;  
 The knowledge which we gain, an illuminating torch  
 And all who seek may perceive and learn.*

*-The Concept of Dragon Seeds*

**CAMINO**

by M. D'Imperio, P16

CAMINO machine dictionary files have become familiar and valued aids to many Spanish, French and Vietnamese linguists and analysts at NSA. The philosophy and design of CAMINO, as originated and developed by Doris Miller, GØ2, and Virginia Jenkins, E13, have been well tested and matured by experience with the Spanish, French, and Vietnamese language files, first on the TIPS PILOT machine processing system, and now on its successor, TIPS I. In the last year some exciting new developments for CAMINO have come on the scene. Many linguists and analysts who might gain from using the existing CAMINO files or some of the new files planned for the near future may be unaware of the possibilities and of the recent major improvement in machine service and response.

What is CAMINO?

CAMINO is a well conceived, proven method for providing mechanized dictionary files. It embodies a very simple, direct, and practical approach that makes best use both of human skills and preferences and of machine capacities and procedures as well. CAMINO owes its special success to three essential features. The first of these is its general design, applicable to any "simple" dictionary file; that is, any file in which a term, a meaning,

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

a security classification, and a source designation will suffice to carry all the separately machine-retrievable items of information desired by the sponsor for each entry.

The second important feature of CAMINO is the benevolent presence of a File Executive: a full-time guardian angel who watches over the file and its users. The File Executive is responsible for the quality of data in the file, and the quality of the services provided. He must be a skilled and authoritative lexicographer and linguist.

The third major characteristic of CAMINO is its simplicity of design. The economy and directness of methods used in CAMINO make data preparation, file maintenance, publication, and provision of various user services routinely feasible in a production-oriented environment. The editing, machining, and correction of input data in elaborate formats has too often become a rock upon which ambitious projects have foundered in the past. By contrast, in CAMINO, the File Executive need not be concerned with intricate systems of codes, designators, line formats, sequences of special fields, or the like, but can instead concentrate on the linguistic and lexicographic essentials in the term, meaning, and source.

#### What Services Are Now Available?

At present there are three language files in full operation under CAMINO. These are: (1) the Spanish Language File (SLF), File Executive Miss Mildred Tasker, G54, phone 4235; (2) the French Language File (FRANCOPHONEGLOS, FPG), File Executive Miss Barbara Dudley, GØ3, phone 5933; and (3) the Vietnamese Language File (RICEBOWL, ), File Executive Mr. Harry Rashbaum, B644, phone 43Ø6.

Another B Group file is the B12 "Jungle Book" which contains six languages: Burmese, Cambodian, Kachin, Karen, Laotian and Shan. File executives for the B12 file are Robert Kreinheder, Joseph Amoroso and CT2 John Francois, phone 4981 or 5278.

Linguists and analysts may query these files on-line (i.e., directly to the computer) through the RYE Mod-35 teletype stations

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

in their areas. Queries may include simple lookups of terms, degarbling, and extension of text to the right and (with a bit more trouble) also to the left. Users of the file are strongly encouraged also to note any new terms and meanings they themselves have recovered and provide them to the File Executive for entry into the file. This two-way flow of information and the participation of users in the growth of the file is a vital part of the CAMINO philosophy.

For instructions on the use of a CAMINO file, consult the File Executive. Linguists and analysts should never hesitate to telephone the File Executive or make a visit to the office. The File Executive maintains a library of printed glossaries, dictionaries, and other aids for the customer, and, as an authoritative linguist and lexicographer, can provide much additional help and advice. The executive undertakes to supplement and complete the purely mechanical facilities of the CAMINO file -- for example, by noting remote queries that did not find an answer researching them, and communicating the findings to the questioner as soon as possible.

The on-line CAMINO machine facilities are now provided by the TIPS I system on the Univac 494 computer, with RYE teletype outstations widely distributed in operational areas. In addition to processing remote queries from linguists and analysts, this system permits the file executive to enter changes or new terms directly into the file as often as desired. This feature allows the CAMINO "on-line" file to be truly up-to-date, so that it faithfully reflects the File Executive's current knowledge.

The other major way that CAMINO files may serve their customers is through printed listings of the file, made periodically by the File Executive and distributed to customer organizations at NSA or in the field, where they may be directly consulted like any other printed material.

The machine listing of a CAMINO file can become very cumbersome to handle and take up considerable storage space. The size and weight can be reduced considerably without an undue sacrifice of readability by requesting a "minitrain" printout. Certain subsets of the terms in the total file can also be selected for printing, by using the security classification (for example,

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

deleting all classified terms), or by using the "source" field (for example, to select all military terms, or all cryptologic terms, etc.).

The bulk listings and selections are made on the IBM 360/85 computer system by C5 at the File Executive's request. The File Executive also uses the same off-line or indirect, mode of access for bulk additions to the file (as, for example, when all terms in a new source dictionary are to be added at once).

#### Machine Service Has Now Improved Greatly

While CAMINO was operating on the TIPS PILOT system, it was plagued by many difficulties originating outside of CAMINO itself, relating to the RYE machine system. These extraneous troubles effectively conspired to hinder or even to frustrate the on-line direct access to the language files by customers which CAMINO designers intended. A number of linguists and analysts who tried to use CAMINO may have become discouraged and abandoned the attempt in disgust, either relying entirely on printouts or rejecting CAMINO entirely. I urge these once-burned, twice-shy potential customers to come back again now for a new experience. CAMINO, under the TIPS I machine system which has taken over from TIPS PILOT, is working on-line now as it was intended to work and as it should have been working all along. Now CAMINO users can realize the full potential of the language files, unhindered by the difficulties that hampered them before.

#### Establishment of P1 CAMINO Committee

Another important new development is the establishment by P1 of a working committee to oversee and coordinate all CAMINO dictionary files in PROD. This committee was set up by Dr. Sydney Jaffe, Chief of P16 (P1's Language and Linguistics Element), with the writer of this article as Chairman. We have attempted to include as members all those concerned closely with any aspect of CAMINO as a whole or with any specific CAMINO file, present or prospective.

~~TOP SECRET UMBRA~~

# ~~TOP SECRET UMBRA~~

## CRYPTO-SCRAMBLE

By Richard Atkinson

Unscramble each of the five numbered crypto-scrambles, placing one letter in each space, to form five words or names, each of which fits the definition to its right.

- 1. A H A R D G I M A T  
 \_ \_ \_ \_  \_ \_ \_ \_  
 Helpful format for recovery of transposition systems.
- 2. T W I T S  
 \_ \_ \_ \_  \_  
 RYE program which decrypts single or double transposition.
- 3. T R A I N I S O N P O S T  
 \_ \_ \_ \_  \_ \_ \_ \_ \_  \_  
 Cryptosystem which does not change the identities of the plaintext characters.
- 4. O D D L E O  
 \_ \_ \_   \_ \_  
 The only RYE program which will produce a crenelated diagram.
- 5. A R A G M A N  
 \_ \_ \_ \_  \_ \_ \_ \_  
 Produce plaintext by rearrangement of the cipher characters.

Now arrange the circled letters to form the cryptoanswer suggested by the cartoon at the right.

Print CRYPTOANSWER here.

\_\_\_\_\_



Answer on Page 43

~~TOP SECRET UMBRA~~

THE IMPORTANCE OF BEING HONEST

by A. L. Gilbert, B6403

In a work situation where the orientation is primarily toward technical expertise, it is natural that every person having managerial responsibility will not necessarily possess management skills. The National Security Agency, in acknowledgement of this, provides a broad managerial development program supplying education in the techniques and factors involved in the supervisory aspects of job performance.

These programs have done a good deal to increase awareness of responsibilities and methods of management. Unfortunately, courage and honesty are traits already developed in an individual personality by the time he becomes a manager, and this seems to be the area where management at NSA most frequently is inadequate.

Honesty is one of the most important elements in any human relationship and is the best way to develop understanding. Everyone is glad to be the bearer of good news, and it therefore travels rapidly through official channels. The transmittal of negative information often travels not at all or through rumors. The supervisor is happy to present a promotion or an outstanding rating but often neglects to inform an employee of qualities in his performance which are hampering his promotability or career development. Presenting a true evaluation of performance in an objective manner, with recommendations for areas of improvement and channels to pursue, can help an employee. Too often, in the atmosphere of close technical interdependence, the supervisor fears that the loss of a personal relationship will result from honest, critical counselling. The opposite is true in most cases, providing the counselling is done with intelligence and consideration.

The deficiencies in the formal evaluation system at NSA (and wherever a similar system exists) make the system useless as a method for counselling. The burden of guidance therefore rests upon the personality of the supervisor and his courage in being honest with his people. It would be refreshing and stimulating to see some progress toward more than superficial concern for employee welfare.

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~CHINA-WIDE TECHNICAL SPECIALISTS: A WAY TO SAVE OVERSEAS

by Stanley Waddell, B41

Because of the current and projected cutbacks in defense spending by the United States, I believe that it is time for DIRNSA, specifically B Group, to think in the same terms. The Defense Department is in the process of reducing and consolidating overseas units, hoping that the existing and future jobs can be done with much less expenditure. I concur in this move.

As I look around the Far East (I am now stationed [redacted]), it appears that B Group continues to follow the approach of individualized specialists in a specific job area. For example, there is a CHICOM [redacted] specialist at [redacted] CHICOM [redacted] specialists at [redacted] 7-48/79, [redacted] specialist at NRRYU, etc. I think that B Group could lead the way in beginning a program for CHINA-WIDE TECHNICAL SPECIALISTS.

The CHINA-WIDE TECHNICAL SPECIALIST would begin his (or her) apprenticeship, say, in B21 and stay in this service element for 3 to 6 months until it is determined that he is familiar with all aspects of the Ground Force problem (similar to the INTERN program but using B Group personnel and not necessarily college graduates). After the completion of tours through B21, B22, B3, B4, and B5, the specialist should be eligible for field assignment. The specialist would be assigned to the NSA office in the country where he is working. For example, a specialist in [redacted] would be assigned to NRRYU to serve as technical advisor to [redacted] USN-25, [redacted]. This would tend to show no favoritism toward a particular service. Moreover, most field stations have a complex mission. [redacted]

[redacted] CHICOM PRINTER, CHICOM VOICE and [redacted] but the civilian technical representative assigned is trained only in [redacted]. A China-wide specialist would be competent in several aspects of the problem.

Candidate-specialists at NSA should probably be attached to an independent support group of some sort so that money to pay these people would not come from B21, B22, etc. This arrangement would also free the specialist from division ties and encourage him to work with any CHICOM analysts in any area of

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

B Group. When the specialist returns from his overseas assignment, he would be able to use his experience in the field in training new people to do the same. There is no doubt that users, and producers (both NSA and the SCA's) stand to gain by use of civilians in the field. But we need desperately to get the most for the buck and we are not doing that now. Through the realignment I am proposing, I can see savings, not only monetary, but also those that we NSA'ers sometimes overlook -- such as collection resource savings, analytic savings, processing and reporting savings, technical exchange savings, and CRITICOMM savings.

In short, I believe we can do the job better and cheaper. What do the readers think?

\* \* \*

## InconSequential Puzzle

Don Ross, B42

Certain words in any language bear sequential relationships, that is, they express concepts which have a logical sequence. The most obvious is the cardinal numbering sequence, the initials of which (in English of course) form the letter sequence - OTTFFSSENT etc. Many other sequences thus formed are not so readily identifiable. Can you guess these?

S M T W T F S

J F M A M J J A S O N D

Easy isn't it? Now try:

U T H T M B T Q P S . . . .

F S T F F S S E N T E T . . . .

Not all sequences are numerically related, how about

M V E M J S U N O.

P T S F F F S.

See answers on page 43.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

STRATEGIC IMPORTANCE OF SHENYANG MILITARY REGION

by Claire D. Smith, B205

Shenyang Military Region consists of the three provinces of Heilungchiang, Chilin and Liaoning. The population is considered to be the most technically proficient in China and represents about 10% of the total population. The majority is Han Chinese with significantly large numbers of Koreans, White Russians, Japanese and Mongol tribal groups.

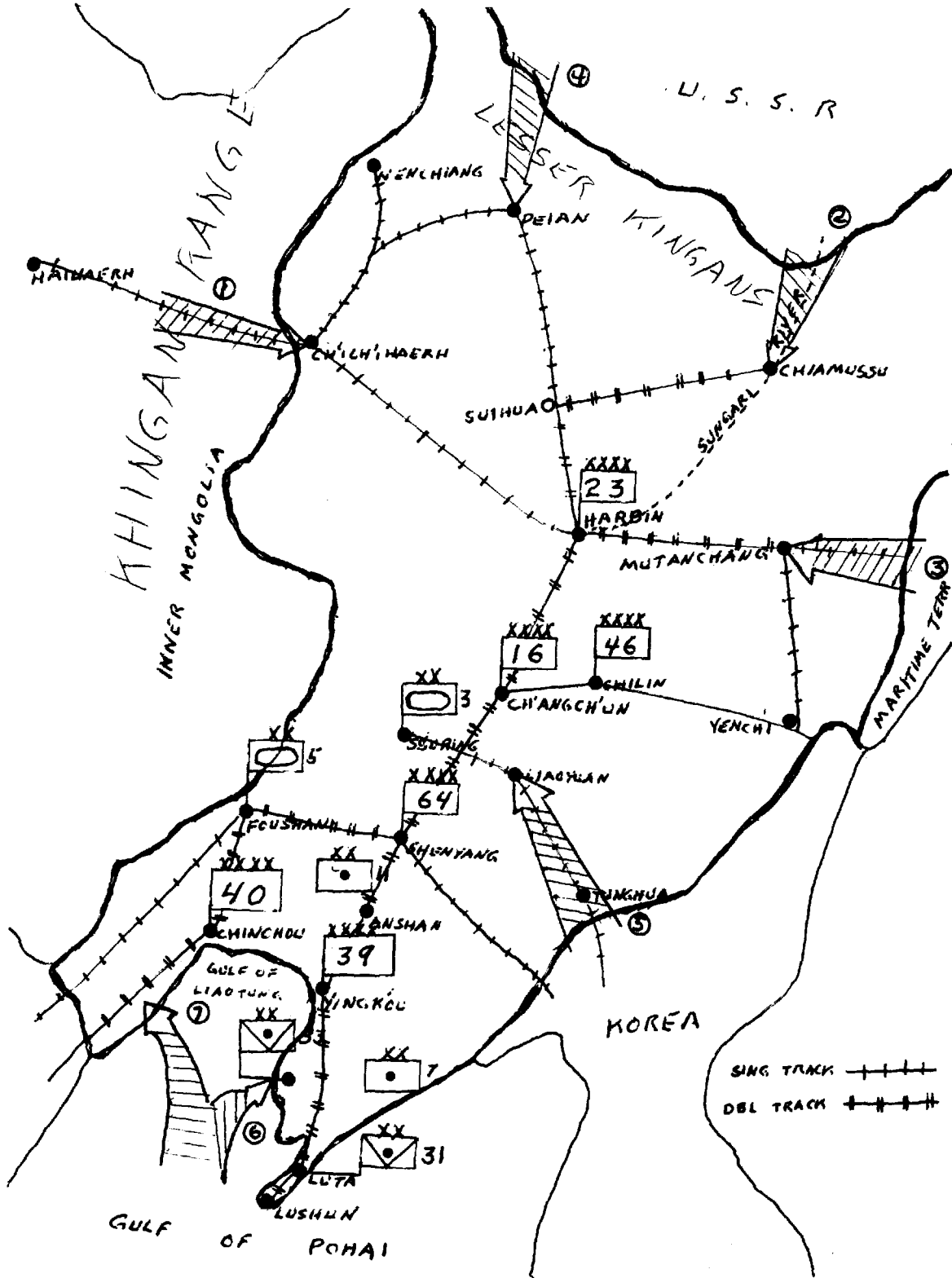
The military region is the richest area in China in terms of resources and industry. Along with a desirable population, it contains vast forests, fertile farm lands, minerals and crude oil. It also has the best railroad and road network in all of China. Two important seaports, Lushun (Port Arthur) and Luta (Dairen), as well as several minor ports are located in the region.

Almost a fourth of China's industry is located within the region, including one of the largest steel complexes in China, a large portion of China's aircraft and electronics industry, and a fourth of the arsenal output.

Defensively, the region commander must be concerned with seven external avenues of approach into the region. Four of these are from the Soviet Union, one from North Korea and two from the coastal areas. Most of them are not too good; however, the CHICOMs must consider each method of approach. (See map.) Three of the avenues of approach were used by the Russians during their invasion of Manchuria in 1945. The first is along the Hailaerh-Ch'ichihaerh railroad which crosses the Greater Khingan Range; the second is along the Sungara River towards Chiamussu and Harbin; and the third is across the eastern highlands in the Mutanchiang area. The fourth route of approach would be across the Lesser Khingan Range towards either Peian or Nenchiang. These avenues of approach involve extended movement through difficult terrain, laying themselves open to guerilla attack and harassment. The avenue of approach through North Korea (5) would also involve operations in difficult mountainous terrain, but, unlike the northern approaches, would not have long distances to traverse in

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

order to reach major industrial centers of the region.

The coastal areas are generally unsuitable for amphibious invasion. Two areas are, however, marginally suitable. The first (6) is along the western tip of the Liaotung peninsula. An invasion in this area would allow limited movement along the narrow coastal plain toward Anshan and Shenyang and in the opposite direction towards Luta and Lushun. The western coast of the Gulf of Liaotung (7) is also suitable for amphibious invasion. Troops landed here could move along the coastal plain connecting the north China and Manchurian plains.

The disposition of Armies within the region leads to the belief that the CHICOMs fear amphibious attack much more than an attack along the northern approaches. As stated before, an attack in the north would involve movement through difficult mountainous terrain, populated by a hostile, guerilla trained, military and civilian force. In addition, Soviet lines of communication would be extended as much as 500 miles before reaching any major industrial center.

In the south, the Chinese have concentrated three armies (39th, 40th, 64th), two of their three antitank divisions (31st, 33rd), two armored divisions (3rd, 5th) and two artillery divisions (7th, 11th). The 16th Army at Ch'angch'un is probably their reserve army, which can be moved either north or south via the excellent double-tracked railroad. The more than adequate naval defense capabilities of the North Sea Fleet must also be considered in presuming the Chinese are thinking in terms of amphibious assault.

\* \* \*

"Who spilled the ink on the Code room floor?"

"DAH-DAH DI-DIT"

~~TOP SECRET UMBRA~~

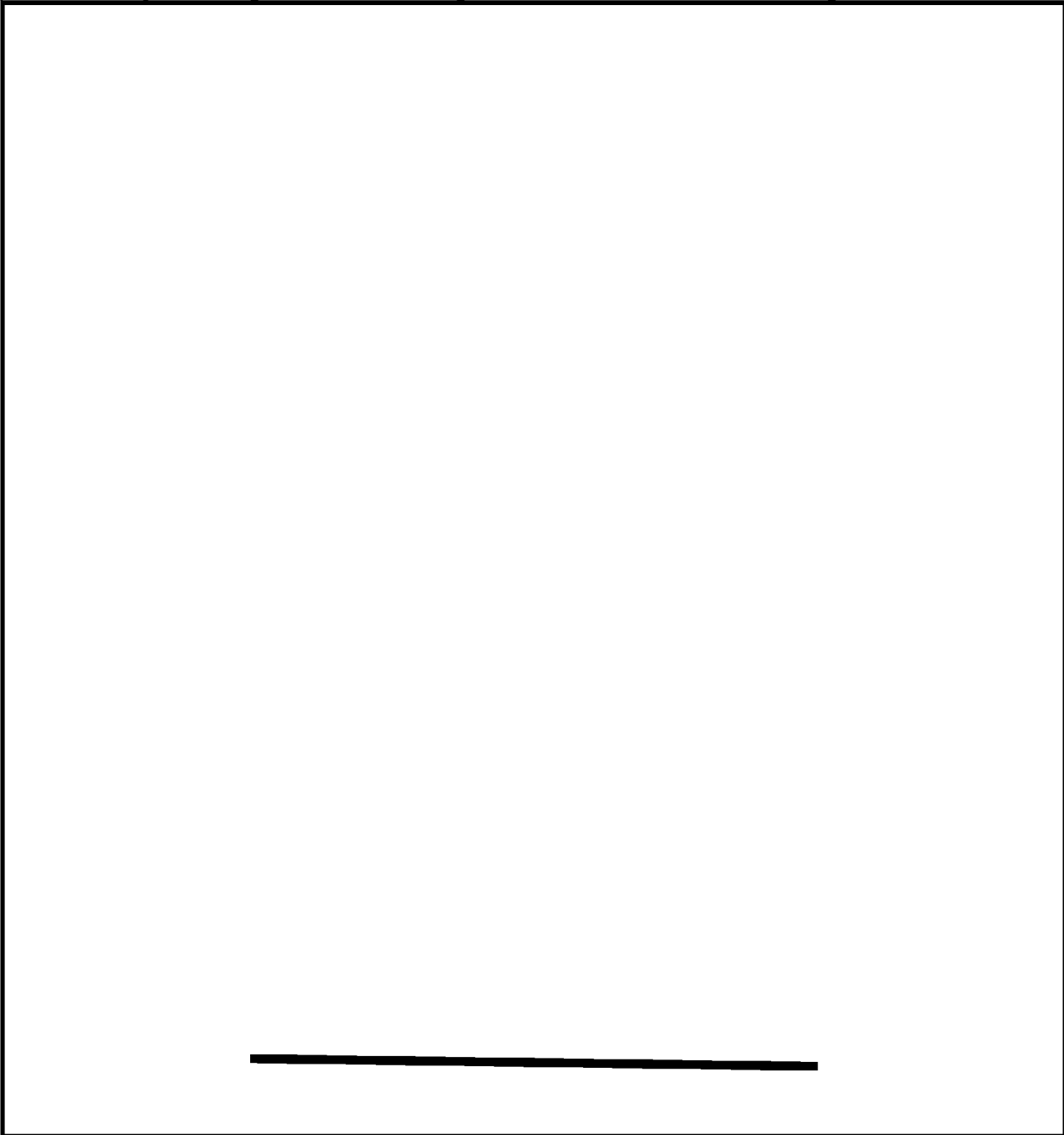
EO 3.3b(3)  
PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~

HOW GREAT COMINT FACTS FROM LITTLE SLIVERS GROW or MAKING  
RUSSIAN MOLEHILLS OUT OF CHINESE MOUNTAINS\*

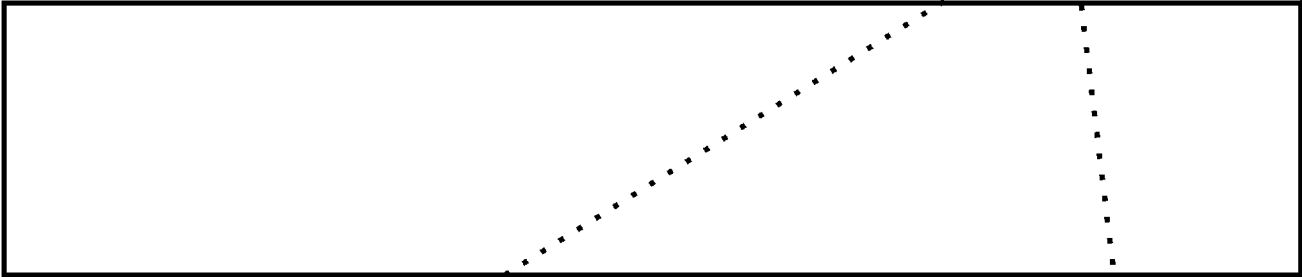
by John J. Mollick, B51

An excellent example of the need for analysts to thoroughly examine even rather innocuous looking messages for hidden scraps of information is a Chinese Communist civil message I encountered a few years ago. The message to which I am referring stated that



~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605



In addition to proving the importance of thorough research of every message (and the incidental fact that Russian appears to be Greek to some Chinese), this brief message was instrumental in helping to prove the Chinese Communists were [redacted] at a time when this was uncertain. Seldom have I had such gratification from working out a Chinese puzzle!

\* \* \*

TO THINK I ATE THE WHOLE THING!

Hong Kong March 17, Reuter -- North Vietnamese doctors have killed a nine-inch long "monster" with head tongue, teeth and legs growing inside a 22-year-old man, the North Vietnamese News Agency reported.

"The monster was located between the liver, the right kidney and the right lung," the News Agency said today.

"It weighed 1.5 kilograms (3 pounds 5 ounces) and measured 25 centimeters (10 inches) in length. It had a monstrous tongue capping the head which had a cyclopic eye and vestiges of the jaw with well formed teeth.

"The neck passes through the diaphragmatic muscle of the subject and links its big head to an imperfect abdomen which has inferior limbs resembling two chicken legs," the article said.

The News Agency said the surgical team in Hanoi was headed by Prof. Ton That Tung, who performed a similar operation on another patient 15 years ago.

The Agency did not identify the patient, nor did it say whether he was feeling any better.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~LETTER FROM PLEIKU

by Tom Glenn, B61

During late 1967 while I was on TDY to Pleiku, Vietnam, I received a most welcome letter from the people I worked with in B6205. They asked me how I liked Pleiku (which Don Jackson describes as the only place in the world that imports mud -- it must to have that much!).

The question brought such mixed emotions that a normal letter could not begin to portray all that I wanted to say. So I wrote a poem, quoted below. Copies of it got into the hands of the Pleiku analysts who like it. One former analyst there, Mike Hricik, now a civilian in B62, unearthed a copy of the poem recently and gave it to me. Things have changed a lot in the last four years, but I gather from recent returnees that the description remains meaningful.

DEAR OSERS,

*Your missive brought me the news  
Of changing aspects and views.  
So I thought I would write you a tale to delight you  
Of impressions uniquely Pleiku's.*

*For my home's now the Central Plateau,  
Where pythons and rodents all grow,  
Where never is heard an encouraging word,  
And progress is painfully slow.*

*The decor can give one the feel  
Of a life more confused than genteel--  
The style is eclectic and tending toward hectic,  
With appointments in barbed wire and steel.*

*But to say that the billets aren't spacious  
Would only be slightly fallacious.  
For those willing to share, there'll be room to spare--  
If you're narrow, short, thin, and tenacious.*

*The problems the housegirls create  
Keep the men in a chaotic state.  
To describe their relations, one needs calculations  
Of the range between loathing and hate.*

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

*The shop is quiet in keeping  
With the intellectual steeping  
Of analysts who express themselves through  
Screams, cries, hoots, yells, and some weeping.*

*But aside from this minor defect,  
Life here gives one pause to reflect  
On the meaning of closeness, the fine points of grossness,  
And the smells that one's mind can't reject.*

*For excitement there's nothing I lack.  
For here I can lie on my back  
And with sheer fascination watch flares in gyration  
With rockets, tube mortars, and flack.*

*And there's always that feel in the air--  
Just knowing the VC are there--  
Armed with such trifles as punjis and rifles,  
With claymores and dum-dums to spare.*

*It's been said and it's well worth repeating  
That the cooks who do all the feeding  
Have tastes so elite it becomes quite a feat  
To tell what it is that your're eating.*

*And the marvellous variety one sees  
Of innumerable types of disease--  
Why there's plague of the thyroid and galloping typhoid  
And something called "Analysts' Wheeze."*

*So with all the advantages here  
The people who stay for a year  
Lead lives quite inspiring, an existence requiring  
Guts, wit, and a well-practiced sneer.*

*I don't mean to say it's not fun.  
It depends on how your tastes run.  
If one of your vices is permanent crises,  
Your search for Utopia is done.*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

WGTS FM (91.9 mc), Takoma Park, Maryland, has been presenting a weekly series called "Hua-yü 'Chieh-mu" (Chinese Language Program) featuring the language and culture of the Chinese people. The half-hour program comes on at 1630 on Thursday and is repeated at 2230 the following Sunday. The language lessons consist of 14 programs introducing simple, common vocabulary and sentences, with half of the program in Mandarin and half in Cantonese. Two musical selections are presented also. When the language series is concluded, Chinese music with commentary is being offered. However, the program director, Dan Lee, advises that the language programs will be repeated later.

\*\*\*

SIGLEX, the Special Interest Group on Lexicography, has been organized under the sponsorship of the CLA. It is dedicated to the broad interests and applications of the field of lexicography at NSA. The group aims to study and investigate the general

principles and practices of dictionary and glossary making, both inside and outside of NSA, with a view to improving current Agency practices and advancing the Agency state of the art.

Monthly meetings involve presentations and discussions on topics relating to lexicography. Also, special projects, such as the preparation of a bibliography of publications on lexicography, are being launched. For further information, contact Bob Kreinheder, 5278s.

\*\*\*

What about post-professionalization C/A training? Have you given any thought as to how you can continue your technical education and enhance your professional background after you have been certified as a cryptanalyst--or did you think that, since you have arrived, there is nothing more to learn? There is a course given in the Agency--the Intensive Study Program in General Cryptanalysis, conducted by Lambros D. Callimahos--that serves as an eye-opener for anyone who thinks he has a well-rounded

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

technical education. The pace is terrific, the amount of instruction jam-packed, and when you finish 18 weeks later, you marvel at the things you learned which you wish you had known before to help you on past operational assignments. A prospectus of the course can be obtained either from P1 or from the Registrar of the NCSch. Better yet, information on the substance and conduct of the course can be gotten firsthand from any of the 200-some cryptanalysts who have graduated from the course during the last 17 years.

Some graduates have expressed an interest in and a need for an occasional refresher course sometime after completion of the Intensive Study Program. The second course could be of shorter duration and perhaps merely highlight the original course. How do you feel about this, Mr. Callimahos?

\*\*\*

B Group's Language Media Center has been established in 3S076. The purpose of this center is to provide a readily visible display of current and future training available to all B Group personnel. In the future the center will also contain a library of language kits, training aids, dictionaries, and periodicals. The information we provide is vital to our personnel for

purposes of advancement and professionalization. If you have any questions regarding language courses and/or training please feel free to stop in and see us, or call 5309.

\*\*\*

The creative endeavors of B Group personnel were very much in evidence in the publicity releases for the CLO Symposium held 6-9 March 1972. The covers of the preliminary announcement and brochure were designed by Minnie McNeal Kenny, B03; Steve Deck, B05, fashioned the eye-catching mobile which graced the foyer of the cafeteria; and it was their combined talents which produced the various posters and flyers heralding the event.

\*\*\*

Did you know that on-the-job training in computer programming for B Group analysts is available through B42? A limited number of analysts detailed to B42 for a period of six months, are trained to use the computer capacity provided by C Group and to program B Group applications for quick-turn-around processing. B1 is currently using this program on an informal basis. Additional information can be obtained from John S. Groat or Donald A. Ross, 5949s.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

The texts of the presentations at the Quality Control Symposium held under P1 auspices during March 1970 and February 1971 have been collected and published in booklet form. Copies can be obtained on request from Harry Rosenbluh, P16, Room 3W090, 5642s.

\*\*\*

Your attention is called to the 26-week television series of film classics to be shown on WETA, Channel 26, every Friday night at 8:30. These films--most of them foreign--carry the original soundtracks, and this is an exceptional opportunity to hear ten foreign languages "in action" without leaving your own home. The CIA urges all local linguists to see at least those films that involve their languages.

\*\*\*

Articles for publication may be submitted through Division Press Corps members or directly to DRAGON SEEDS, B03.

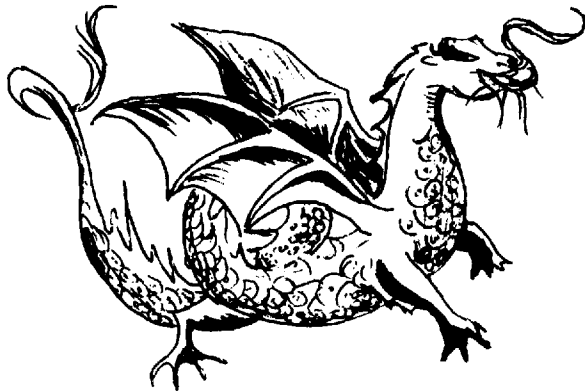
PROD TECH BRIEF

Nearly every Tuesday morning at the PROD TECH BRIEF, analysts have the opportunity to brief the top echelons on significant technical developments. B Group personnel have participated in two recent PROD TECH BRIEFS: on 8 February 1972, Jim Watson of B21 spoke on "Chicom [redacted]" on 21 March 1972, Ken Cohen of B45 presented a briefing on "Solutions to Chicom [redacted]"



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



ASK  
THE  
DRAGON  
LADY

Dear Dragon Lady:

Those of us working with the so-called "exotic" languages operate under a considerable handicap, due to lack of language training and language aids.

For example, I work with a language in which I was trained for only two months because the only native speaker of this particular language in the country has left the Washington area for a post at the University of Indiana. At the present time my language aids consist of one dictionary printed in 1906 and a running card file. At best, such language aids cause considerable gaps in my product. At worst, they lead to misinforming the consumer.

It may be that NSA cannot afford to send analysts all across the country to track down competent instructors. But NSA could contract such instructors, either directly or through a third party, to compile language aids peculiar to agency needs.

WILLIAM A. DE GREGORIO, B12

Dear Dragon Lady:

With all the emphasis on professionalization and the development of the "complete linguist," please tell me what efforts are being made to provide advanced training in the minor tongues? Senior Russian linguists are fine-tuned by tours to the U.S. Army Institute of Advanced Russian Studies in Garmisch-Partenkirchen, Germany; Chinese linguists can study at the U.S. Embassy School for Chinese Language and Area Studies

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

in Taichung, Formosa; and Durham University (England) serves as a finishing school for students of Middle Eastern languages. But what about Cambodian, Korean, Thai, Vietnamese, Lao, or Burmese linguists? Couldn't similar arrangements be made at the University of Hawaii? Or what about universities in Bangkok, Paris, Phnom Penh, Rangoon, Saigon, or Vientiane? Nothing beats studying a language in its native habitat or in a locale where colonies of native speakers live.

NANG HA'NYAN, B03

Continuing her policy of having letters and questions answered by the most authoritative sources, Dragon Lady has solicited the help of Dr. Sydney Jaffe, Chairman of the Language Panel, to answer the above letters:

I have your letters to Dragon Lady about training in Asiatic languages.

The questions are excellent ones, and I intend to pursue them. I can only say now that we have no plans to send people to Hawaii, Saigon, etc. But that's not the last word.

Within the next few weeks, I am going to conduct a complete review of training needs, language by language. That will be the time to decide what we want to do. When that process is complete, I'll be better able to answer your questions.

SYDNEY JAFFE, Chief, P16

\*\*\*\*\*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Dear Dragon Lady:

Is it true that the Language Career Panel is about to initiate an inter-agency exchange program for language interns? If so, let me offer my support for such a program and briefly discuss what I think some of the benefits would be.

A greater understanding could be created between sister agencies such as NSA, CIA, DIA, and State Department of language problems peculiar to each agency. Solutions could be found on a more timely basis, thereby rendering U.S. intelligence operations more effective.

Not only could the language intern increase his knowledge of and capability in a specific language, but he could become much better versed in the activities and functions of the other members of the intelligence community. NSA would be gaining a more insightful and effective employee.

Since it is admittedly difficult for language interns to tour different areas of NSA, as other interns do, an inter-agency exchange program could go a long way toward stimulating the language career field.

I hope such a program can be worked out for the benefit of the entire intelligence community.

FLORENCE WAGNER, B12

Dear Florence:

Indeed, such a program is being investigated by the Language Career Panel. However, nothing concrete has been decided. Be assured that if and when something definite is determined, the program will be announced to the general public.

DRAGON LADY

\*\*\*\*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Dear Dragon Lady:

What's Tirzah Clark doing these days?

M. I. REED, B44

Dear MIR:

Since her retirement in 1970, Tirzah Clark, formerly of B65, has become a world traveler. For those of you who know her, we publish extracts of a letter sent from Kyoto to Dot Evans of B65 telling of her travels.

DRAGON LADY

*"The villages around Pusan are enchanting clusters of six or eight houses, surrounded by trees, with faded rose or blue tile or thickly thatched roofs. I couldn't get a photo from the car, and the rather inferior postcards are all of cultural treasures. We went to a most unlikely temple on a hill, set against gorgeous pines with red trunks; the pillars, eaves, and monsters at the corners recall Sicilian carts, but so delicately that the effect is not garish. Then back to Kobe, where Holly and I brought our heavy suitcases here.*

*Then to Nagoya, where we stayed three days because rain held up the loading. The first afternoon Mrs. Watanabe, the wife of the Everett manager and an Ikebana teacher, her assistant (I gathered, nobody but the agent spoke English), and two adorable girls, dentists' assistants, came in with masses of roses, chrysanthemums, cockscomb, fern, crotons, and what all, to give first a demonstration of flower arranging, then of the tea ceremony. The next day, Sunday, the two girls gave up their day off to take the rest of the party to a nearby village where there was a pottery fair. A madhouse, I gather, but people managed to struggle through to enough stalls to come back laden. The two girls stayed for dinner, and I managed to put together two Japanese sentences from the glossary and be understood!*

*The thing that has constantly amazed me is the non-touristy nature of Japan and Korea. In both, we are almost always the*

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

*only Caucasians in sight and are gawked at as much as a Japanese tourist would have been in a small town in the '20s. In Korea, it went beyond that. On the trip from Pusan, Natalie Golay, a blonde seven-year-old with enormous blue eyes, was repeatedly pounced on and asked to pose for photos, either alone or with a family group of some sort. Far more often than we asked the pretty women in their very becoming native dress--moreso than the Japanese kimono, I think, though what it says for a country's history when its women's dress is based on the theory that a victorious army won't rape pregnant women!--to pose for us. This hotel is popular with tours, so there are plenty of westerners here, but according to one of them I breakfasted with, they are herded from one sight to another and never, never eat in a native restaurant, where Holly and I always eat.*

*My deteriorating handwriting is due to writer's cramp from chopsticks, as well as the pen! I still have to think about it steadily, but I can use them ungracefully enough..."*

(Editor's note: Tirzah Clark--for the benefit of those who did not know her--is something of a legendary figure. She was a brilliant cryptolinguist during her years at NSA. She has been described as something like a cross between Auntie Mame and Margaret Meade. According to some witnesses, she used to translate French-language messages at the typewriter--without bothering to decrypt them--into superb English. )

.....

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Dear Dragon Lady:

Having read Dick Curtin's article "Analyzation of Data," I can only say, "Joy to the World." I have always believed that it is the prerogative of the individual analyst to perform a cursory inspection and follow an intuitive avenue of attack before methodically working for a solution in the manner prescribed by the post-World War II cryppies. This is not to say that these procedures are passé, but rather that we should not close our minds to new ideas and new talent even if they appear awkward. My work has often been scrutinized for these very reasons.

As for getting one's hands dirty, how many times have I heard people say that the sorting and the logging of traffic is a menial task and it is not part of one's job as an analyst to perform such details? But if they only realized that herein lies the smoldering guts of cryptanalysis, I believe our production would increase significantly.

One other item - I feel that certification is helping to alleviate our adaptability problem through the intern panels and the requirement for diversification.

I thoroughly enjoyed Dick's article, but he should brush up on his punctuation. Your publication, for the most part - (I haven't read it completely yet, but I am sure it is the same over-all) was well worth whatever time and effort was required for production.

BOB REIFSNIDER, E/3

P.S. In answer to Dave Shepard's question on terminology, could the Guru have contradicted himself?

From the mouth of the Guru of the Dundee Society come the following words of wisdom:

"In the Basic Cryptologic Glossary, page 3, biliteral substitution cipher is defined as 'a substitution cipher in which the ciphertext units are pairs of characters.' Not a

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

blessed thing is said about the plaintext equivalents, which could be single characters, pairs of characters, or for that matter, even the vocabulary of a small code system."

As for Dick Curtin's article, Bob, did you *analyze* the data?

\*\*\*\*

"The fourth of the paths leading to nirvana is called aya or ayahat. The ascetic who has entered this path is called a Rahat; he is free from all cleaving to sensuous objects. Evil desire has become extinct within him, even as the principle of fructification has become extinct in the tree that has been cut down by the root, or the principle of life in the seed that has been exposed to the influence of fire. The mind of the Rahat is incapable of error upon any subject connected with religious common subjects, or from allowing the faculty of observation to remain in abeyance."

--The Manual of Buddhism

*It sounds like a deadly dull condition to achieve:*

*"A Rahat  
I'm not!"*

----or: *"It's more fun being Jewish!"*

--L.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

## CONTRIBUTORS

MARY E. D'IMPERIO, P16, is a graduate of Radcliffe College and holds the M.A. in Structural Linguistics from the University of Pennsylvania. Scientific linguist, programmer, and data systems analyst, her career with NSA dates from 1951. She is well known throughout the Agency as the author of numerous articles on programming languages, data processing applications and information retrieval which have appeared in the NSA Technical Journal and in scientific journals in the "outside world." She is Chairman of the CAMINO Committee and Vice Chairman and Secretary of the CLA Special Interest Group for Computer Applications in Linguistics.

AL GILBERT, B6043, came to NSA in 1966 after retiring from the Army Security Agency as a CW3. While in ASA, he served in Europe, the Far East, Southeast Asia, and at NSA, working at various times as reporter, traffic analyst, Russian linguist, and cryptanalyst. Mr. Gilbert, who is professionalized as a Special Research Analyst, has worked on the Vietnamese Communist military problem since 1966.

TOM GLENN, Deputy Chief, B61, has a total of 13 years experience with ASA and NSA on the Vietnamese problem. He is a professionalized special research analyst and Vietnamese linguist who has also studied Chinese and French on his own. Mr. Glenn has served as the Chairman of the Vietnamese Language Professionalization Examination Committee. Assigned to Vietnam in 1962-65, 1967-68, and 1969, he has been involved in traffic analysis, cryptolinguistics, intelligence analysis, and most significantly, in the management of the SIGINT reporting effort on the Vietnam war.

JOHN J. MOLLICK, B51, studied Mandarin Chinese at Yale University Institute of Far Eastern Languages in 1955-56, and then served as intercept operator, voice transcriber, and traffic analyst with the USAFSS in Korea until 1958. His NSA (and B Group) civilian service stretches from 1959 to the present, punctuated by an academic year (1966-67) of advanced Chinese area and language studies at the U.S. Foreign Service Institute in Taichung, Taiwan. Mr. Mollick is certified in the fields of language (Chinese) and SRA, and is a frequent contributor of Chinese language articles to the Quarterly Review for Linguists. His present position is Chief, B512, CHICOM Identification Branch.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

MICHAEL J. NUGENT, formerly of B45, entered the cryptologic field as an NSA civilian in 1963 following his graduation from the Baltimore Polytechnic Institute. From then until late 1971, he was a traffic analyst engaged successively on the Soviet, Soviet Satellite, North Korean [redacted] targets, and finally with the CHICOM [redacted] problems. Mr. Nugent's present assignment is collection research technician in W65, Radio-Wave Propagation Prediction Branch.

GEORGE PATTERSON, B653, has been in the cryptanalysis field since 1963 and has worked on Soviet machine ciphers and Laotian Guerrilla (Pathet Lao) and Vietnamese Communist high-grade manual systems. His earlier experience includes two years with NSA as a signals conversion technician and three years in the Army Security Agency as an intercept operator and supervisor.

PHILIP REMSBERG, B41 Machine Applications Project Team, majored in industrial psychology at Gettysburg College and Penn State University. He entered on duty with NSA in 1966 after having completed a three-year tour with the Army Security Agency. Within B41, Mr. Remsberg has worked as a traffic analyst, callsign analyst, and practice systems analyst, with special attention to machine applications against his target problems. He is now engaged in information design studies specifically concerned with the impact of AG-22 on B41 operations.

CLAIRE SMITH, B105, began his cryptologic career at Vint Hill Farms in 1944 and commanded a Radio Intelligence platoon in the Asiatic/Pacific Theater until released from the service in 1946. He resumed his military career with the Army Security Agency in 1948, serving in various cryptologic capacities in Korea and Japan until 1953, when he was assigned to his first tour with NSA at Arlington Hall. There followed a tour in Europe; return to the "land of the round doorknobs" in 1960; and a final military assignment with the S Organization. Mr. Smith's civilian service with NSA began in August 1964 following his retirement from the Army. He was a SIGINT reporter in B21, CHICOM [redacted] until 1968, when he accepted his present assignment in B205.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

STANLEY L. WADDELL, the B41 CHICOM Technical Representative at NRRYU, Okinawa, entered on duty with NSA in January 1952. He worked as a traffic analyst on the Soviet problem until 1954 and on the CHICOM problem thereafter. He was in charge of the CHICOM isolation and identification effort at JSPC from 1965 to 1967 during which time he developed several new isolation and identification programs which are still used in B41. Mr. Waddell served as the first Chairman of the JSPC Civilian Welfare and Recreation Organization from 1966 to 1967 and has been an enthusiastic participant in various NSA sports programs as a player or game official.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

ANSWER SHEET

Answer to Inconsequential Puzzle

1. Days of the week
2. Months
3. Units, tenths, hundreds, etc.
4. First, second, third, fourth, etc.
5. Planets
6. Poker hand:

Pair, three of kind, straight, flush, four of a kind, straight flush

Answer to this month's Crypto-scramble

1. Hat diagram
2. Twist
3. Transposition
4. Doodle
5. Anagram

Cryptoanswer-isolog

Answer to first Crypto-scramble

1. Biliteral
2. Bipartite
3. Digraphic
4. Variants
5. Diana

Cryptoanswer-additive

There have been many comments and queries regarding the article, "Analyzation of Data," by Dick Curtin, which appeared in the November issue of *Dragon Seeds*, but the only solution of record is the one submitted by Chuck Bubeck, B62:

"Alphabetized blather! Curtin's *Dragon Seeds* essay fostered groans hereabouts. I just know large multitudes never overcame paralysis. Quite reasonably surprised to uncover variation within. XXVI? Yeah! ZAP!!"

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

You probably observed the absence of a sentence beginning with the letter "E" and, in fact, the absence of the letter "E" anywhere in the article.

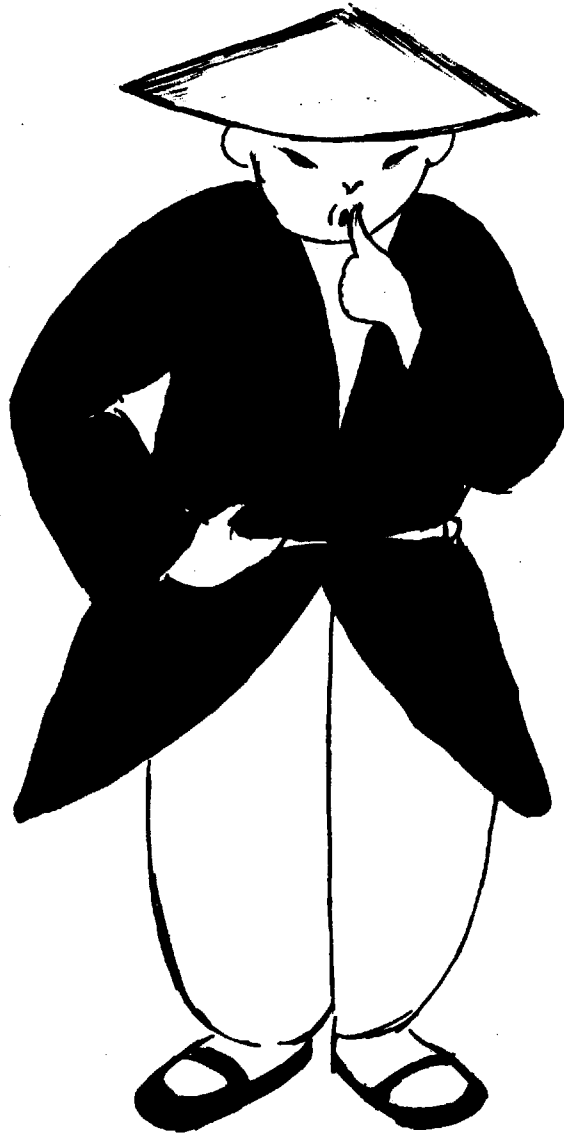
The intent was to see if readers could make certain observations while reading an article concerned with making certain observations. Once the theme of the article was decided upon, the letters A through Z (less E, of course,) were written vertically and sentences were formed beginning with each of the letters. The sentences were then taken in order and grouped to form fairly equal sized paragraphs.

Incidentally, there is a book titled *Gadsby*, written by Ernest Vincent Wright and published in Los Angeles in 1939, which is a novel of about 50,000 words and doesn't contain a single occurrence of the letter "E". (Ref Military Cryptanalysis, Part I, p. 31 footnote.)

~~TOP SECRET UMBRA~~



**Shhhhhhhhhhh...**



*it's classified!*

JUN 72

~~TOP SECRET~~

# National Security Agency

Fort George G. Meade, Maryland



# DRAGON SEEDS

~~APPENDED DOCUMENTS CONTAIN  
CODEWORD MATERIAL~~

~~TOP SECRET~~

~~TOP SECRET UMBRA~~

This is *Dragon Seeds*.

There is fantasy, irony, and the bite of reality in the name. It speaks of the East. And, like the East, it suggests much, says little.

*Dragon Seeds* is both Mother China and her neighbors. *Dragon Seeds* is monumental and minuscule. It is the past and future. It begs for elaboration but gives none. In it are echoed softly slurred Mandarin, brittle Vietnamese, determined Korean. In it is the spectre looming over the Thai, Lao, and Khmer. It is frightening and friendly. It is uncertain.

Above all, *Dragon Seeds* is promise. It is fertile with ideas unbounded, to be cultivated with creativity and imagination. It is challenge. It is alive. It will be more than it is.

*Dragon Seeds* is yours. May it grow with you.

The Editors

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

PL 86-36/50 USC 3605

## DRAGON SEEDS

## Publisher

DONALD E. MC COWN, CHIEF B03

## Managing Editor

Minnie M. Kenny

## Feature Editor

Richard V. Curtin

## Rewrite Editor

Victor Tanner

## Executive Editor

Robert S. Benjamin

## Biographical Editor

Jane Dunn

## Education Editor

Marian L. Reed

## Special Interest Editor

Ray F. Lynch

## Composition

Helen Ferrone

Lorna Selby

## PRESS CORPS

B11 Carolyn Y. Brown

B12 Philip J. Gallagher

B21 Gary Stone

B31 Jack Spencer

Thomas M. Beall

B32 Jean Gilligan

B33 Louis Ambrosia

B34 Thomas L. Wood

B41 James W. Schmidt

B42 Peggy Barnhill

B43 Mary Ann Laslo

B44 Jack L. Thomas

B45 John E. Uzarek

B5 Paul M. Hoagberg

B62 

B63 Allen L. Gilbert

B63 William Eley

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



Vol. 1  
Nr. 3

June 1972

**TABLE OF CONTENTS**

The Chiefs of Staff		2
Maybe It's Related to the Phase of the Moon	Herb Guy, B45	5
The Reality of Communications Changes	E. E. Orr, B41	13
A Need for A Centralized Transcription Operation	Richard S. Chun, B44	17
The Open Door: The Role of Mathematics in C/A	Dr. Ralph W. Jollensten, P1	19
Machine-Aided Translation	Norman Wild, B03	23
Study of ZFK Message Activity	Kenneth Miller, B43	27
Vietnamese Communist Tactical COMINT Operations	Tim Murphy, B6	32
Seedlings		34
Ask the Dragon Lady		36
Contributors		39

~~TOP SECRET UMBRA~~

CHIEFS OF STAFF



E. LEIGH SAWYER  
CHIEF, B02



DONALD E. MCCOWN  
CHIEF, B03



DELMAR C. LANG  
CHIEF, B04



JOHN B. CALLAHAN  
CHIEF, B05

~~TOP SECRET UMBRA~~

"Like men crossing streams in the winter,  
How cautious!  
As if all around there were danger,  
How watchful!  
As if they were guests on every occasion,  
How dignified!  
Like ice just beginning to melt,  
Self-effacing!  
Like a wood-block untouched by a tool,  
How sincere!  
Like a valley awaiting a guest,  
How receptive!  
Like a torrent that rushes along,  
And so turbid!

--Lao Tzu

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605E. LEIGH SAWYER  
Chief, B02

E. Leigh Sawyer has been with the Agency for 21 years. He was recalled to active military duty with AFSA in 1951 and converted to civilian status two years later. In 1957, he left his assignment as Executive Officer of the Director's Plans and Operations Staff and transferred to the ACOM Techniques Group. In this capacity, he was directly involved in establishing the foundation of the emerging Chinese Communist [redacted] problem. Following a two-year tour as NSAPAC Okinawa from 1959 to 1961, he was detailed to serve as the Agency JSPC Project Officer, and authorized by the Director to act independently in behalf of all echelons as a means of accelerating activation. Upon completion of this project in late 1962, he was assigned as Deputy Chief of the Office of European Satellites. In 1965, at the personal request of ADP, he was reassigned as Chief of B21, Chinese Communist [redacted] and remained in this position until 1968. Since that time, he has served as Chief of B02.

Mr. Sawyer graduated from Harvard University in 1943 with a B.A. degree and subsequently, following military service in China during World War II, received his M.A. degree from the Fletcher School of Law and Diplomacy. Prior to his recall to military service in 1951, he taught history, government, and international relations for three years at the University of Connecticut.

\*\*\*\*

DR. DONALD E. McCOWN  
Chief, B03

Dr. McCown's SIGINT career began when, as a graduate of the Infantry OCS at Ft Benning, he was assigned to Arlington Hall in September 1942. In 1944, he was transferred to the London Headquarters, then to Paris and finally to Russelsheim. Dr. McCown spent the winter of 1945/46 at Bletchley, and left this business in the spring of 1946. After an interregnum, he returned to NSA in November 1956, spending nine years in A5, then several as Chief B4, and more recently as Chief B03.

Dr. McCown's previous career was as a Near Eastern archeologist. His study of chemistry at the University of California, Berkeley, was interrupted by two years in Palestine

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

in 1929. He started archeology there and in Trans-Jordan, and in 1933 joined the Oriental Institute of the University of Chicago. Five years were spent at Persepolis in Iran, and then a PhD was achieved just before World War II. A Guggenheim Fellowship in 1946/47 provided a fascinating winter in New Delhi, the Indus Valley, Iraq, and Iran. Dr. McCown then spent two winters in Iran, combining in 1949 the opening of a major expedition at Nippur in Iraq. As Director and an Associate Professor, he continued there until 1954, when he finished necessary publications before returning to the research field he had found so fascinating in wartime.

\*\*\*\*

EO 3.3b(3)  
PL 86-36/50 USC 3605

DELMAR C. LANG  
Chief, B04

Mr. Lang spent 23 years in the Air Force, 16 of them with the USAF Security Service, prior to retiring in August 1965. He is a 1949 Chinese language graduate of the one-year Army Language School course and was instrumental in establishment of the specialized Chinese Language Training Program for USAFSS.

Highlights of his career in the SIGINT community include 14 months in Korea in 1952/53, during which time he pioneered the use of SIGINT in support of tactical air operations; two tours as Officer-in-Charge of the Chinese and North Korean [redacted] Branch of the AFSS Field Processing Center; 15 months as Operations Officer at USA-57, during which time the squadron established the operation which became USA-69 at [redacted] a tour as the Group B Staff Representative at Hq NSAPAC, Camp Fuchinobe, Japan; and a tour as Chief, NSAPAC Representative, [redacted]

His assignments at NSA have encompassed varying tasks in B3 including a stint as Deputy Chief; Deputy Chief, B5; and Chief, B05 from 1963 to late 1967. In the latter assignment, he was deeply involved in the application of SIGINT in support of tactical forces in Southeast Asia.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(6)  
PL 86-36/50 USC 3605

JOHN B. CALLAHAN  
Chief, B05

John B. Callahan's involvement with SIGINT spans 24 years and three continents. It started in 1948 with his military assignment in the Army Security Agency at Herzo Base, Germany, and continued when he joined NSA in March 1953 as a civilian traffic analyst and reported on the Soviet Military problem. Three years later, he was back in Europe as analyst and consultant with CIFCO, the Army Centralized Program. His return to NSA and the Soviet [redacted] problem came in 1959, and for the next six years, Mr. Callahan held various SIGINT reporting and consumer relations positions with PROD Group A. To highlight this period, he helped establish and maintain the Group A Watch Center in response to the Cuban Crisis of 1962. September 1965 found him detailed to the DIA Intelligence Support and Indications Center, where he spent a year interpreting SIGINT matters for this major user.

Mr. Callahan's SIGINT attention shifted to the Far East in September 1966 with his assignment as Chief, Intelligence Staff Group, Office of Communist Southeast Asia. A natural development from that job was a move to Vietnam, where he spent another year providing interpretive support of SIGINT product at DoD Spec Rep, MACV. Back once more at NSA, he became Chief first of B12 (SEA Non-Communist Nations) and then of B11 (Korea). He assumed the position of Chief, B Group Intelligence Staff, B05, in January 1972.

\* \* \* \*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

MAYBE IT'S RELATED TO THE PHASE OF THE MOON...

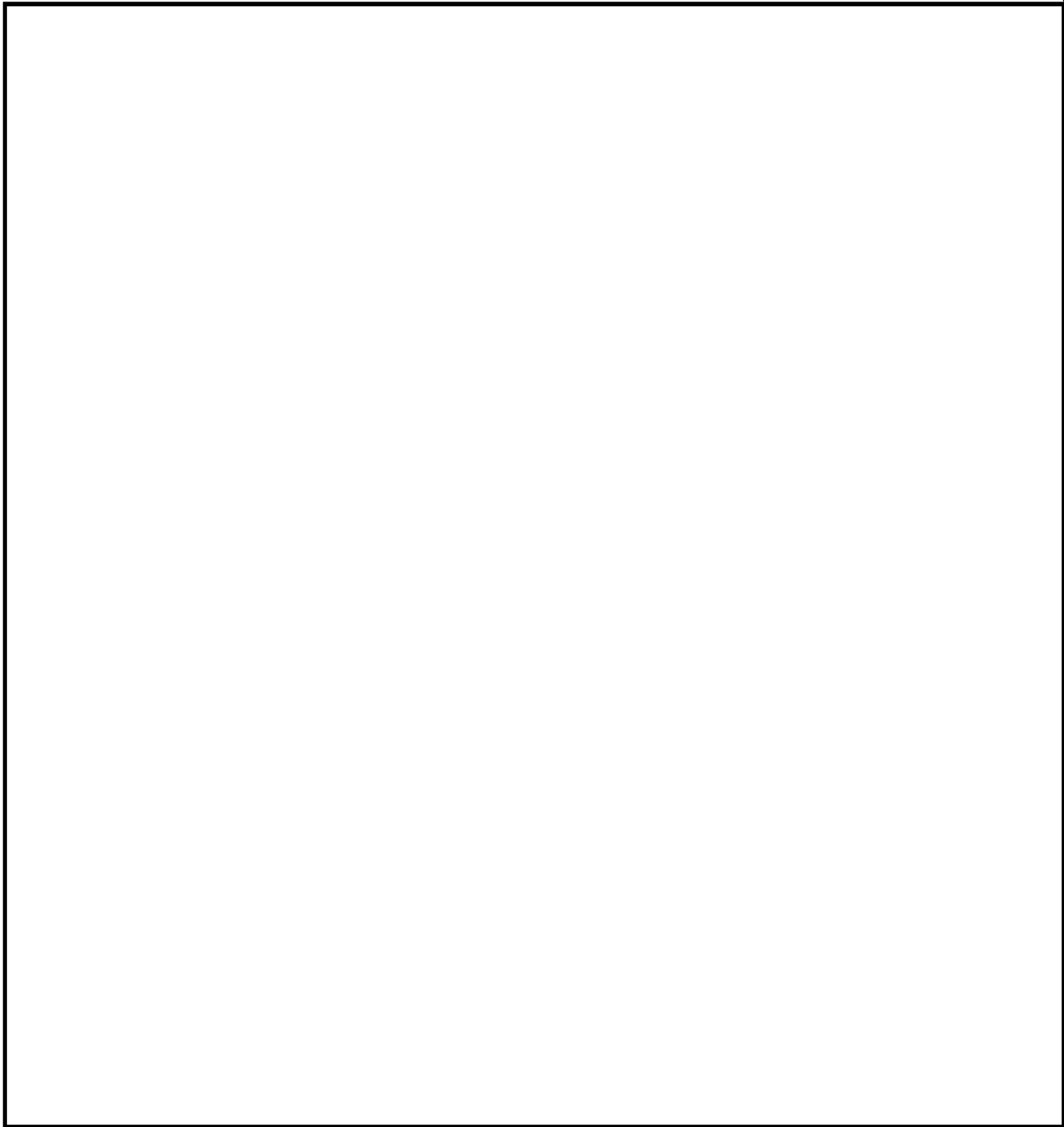
by Herb Guy, B45

This story of the dissection of a callsign system proves the validity of that old saw, "Many a true word is spoken in jest." It proves a lot of other things, too--among them that it ill behooves the cryptanalyst to dismiss the word spoken in jest too quickly. But you may ask what a cryptanalyst is doing "dissecting" a callsign system in the first place--isn't that a job for a traffic analyst? Well, in case some of us haven't yet learned the lesson that you can't really draw a line between the work of the cryptanalyst, the traffic analyst, and the linguist, this story provides a bit more proof of that, too.

The reader has probably guessed by now that the title of this piece was the "true word spoken in jest." But it wasn't really spoken entirely in jest, because we knew that many of

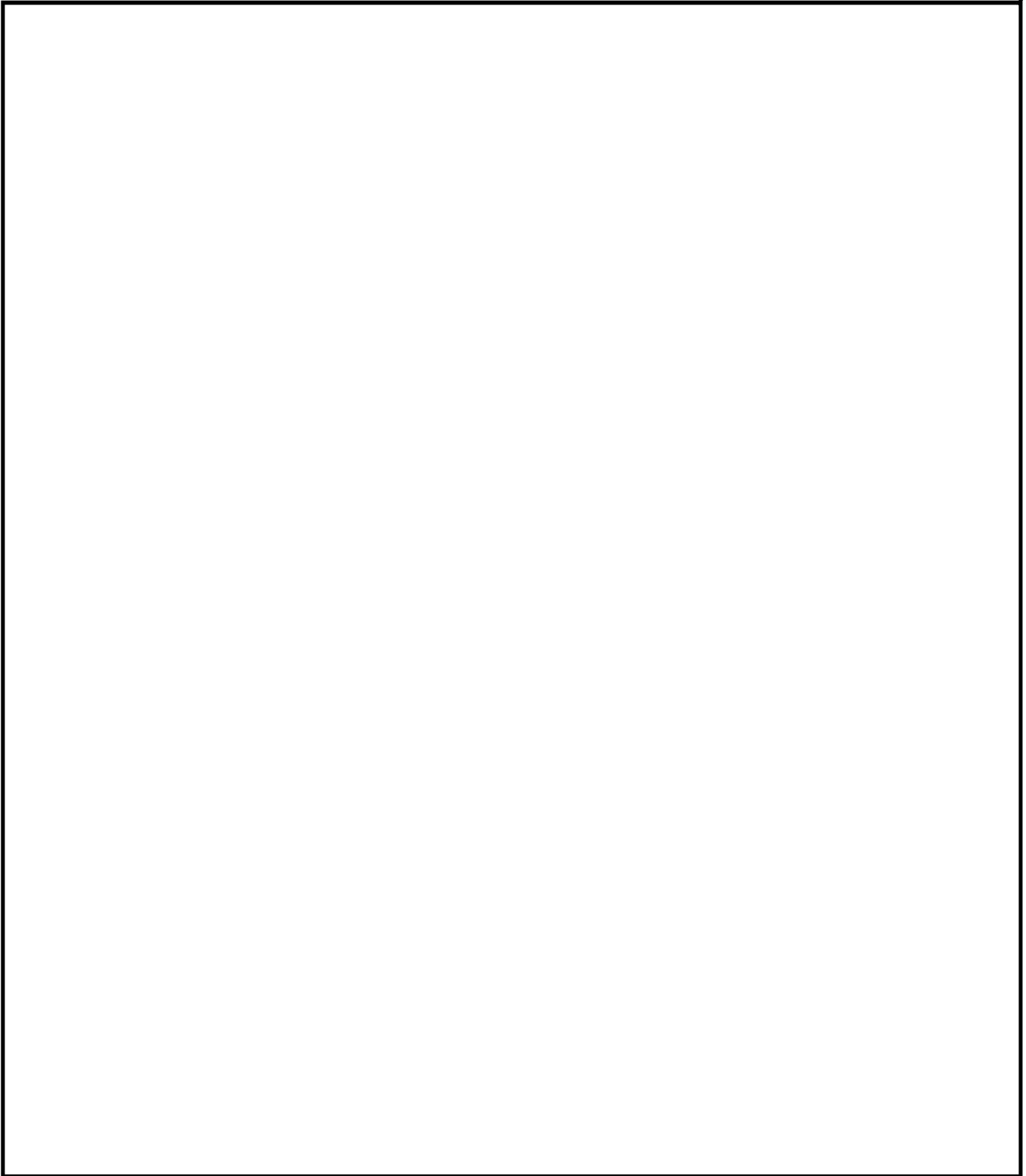
~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



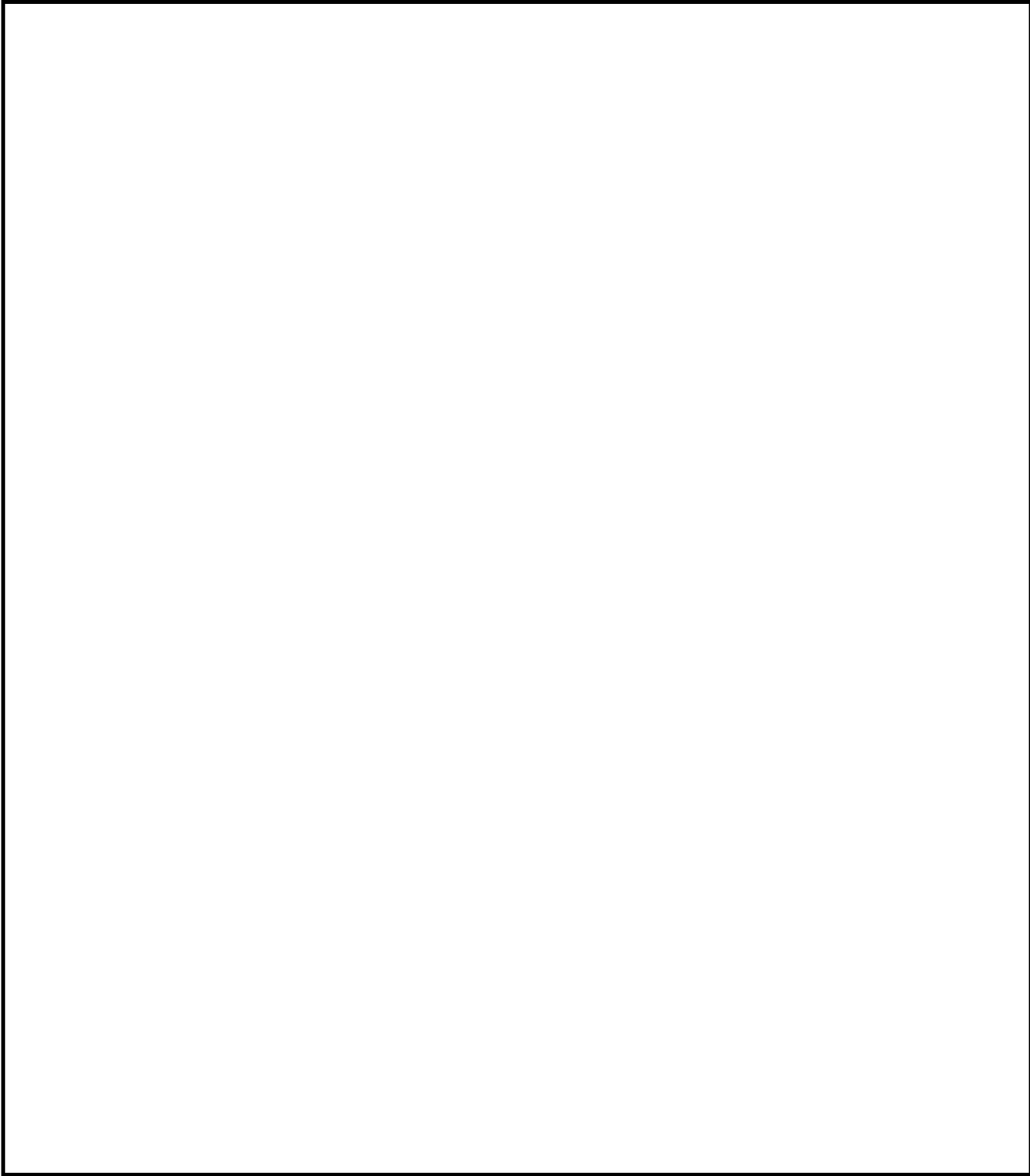
~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



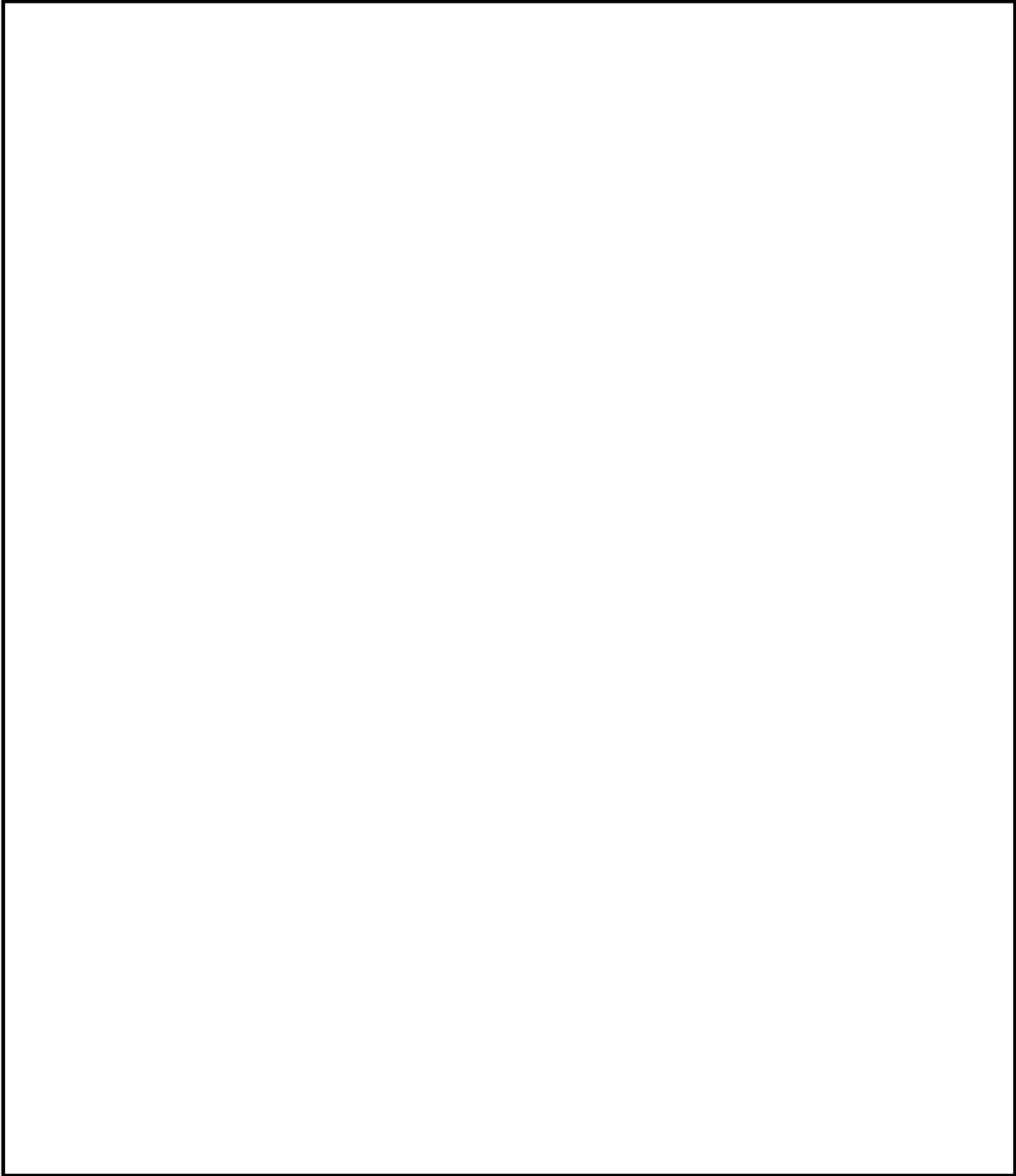
~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

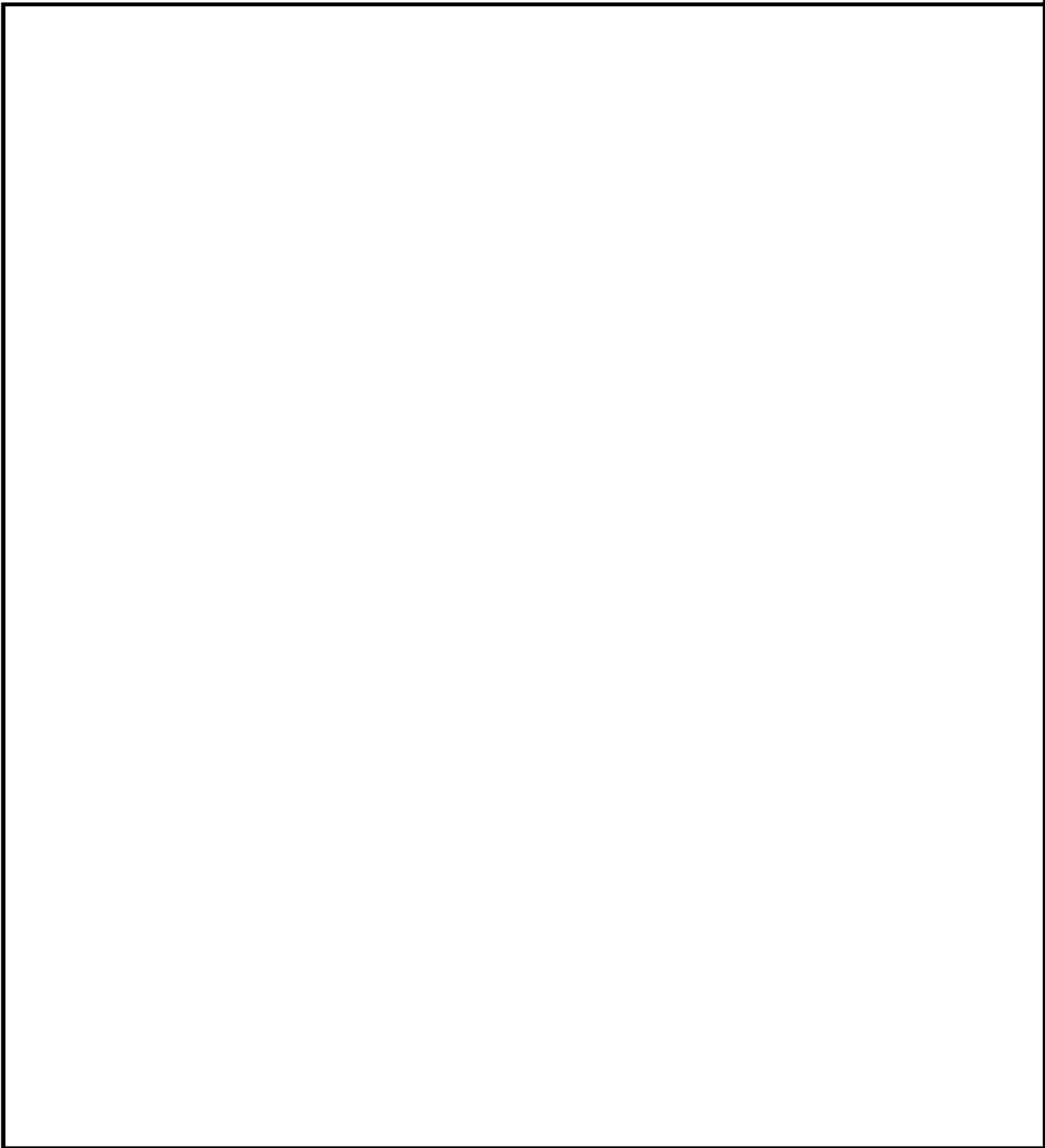
~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

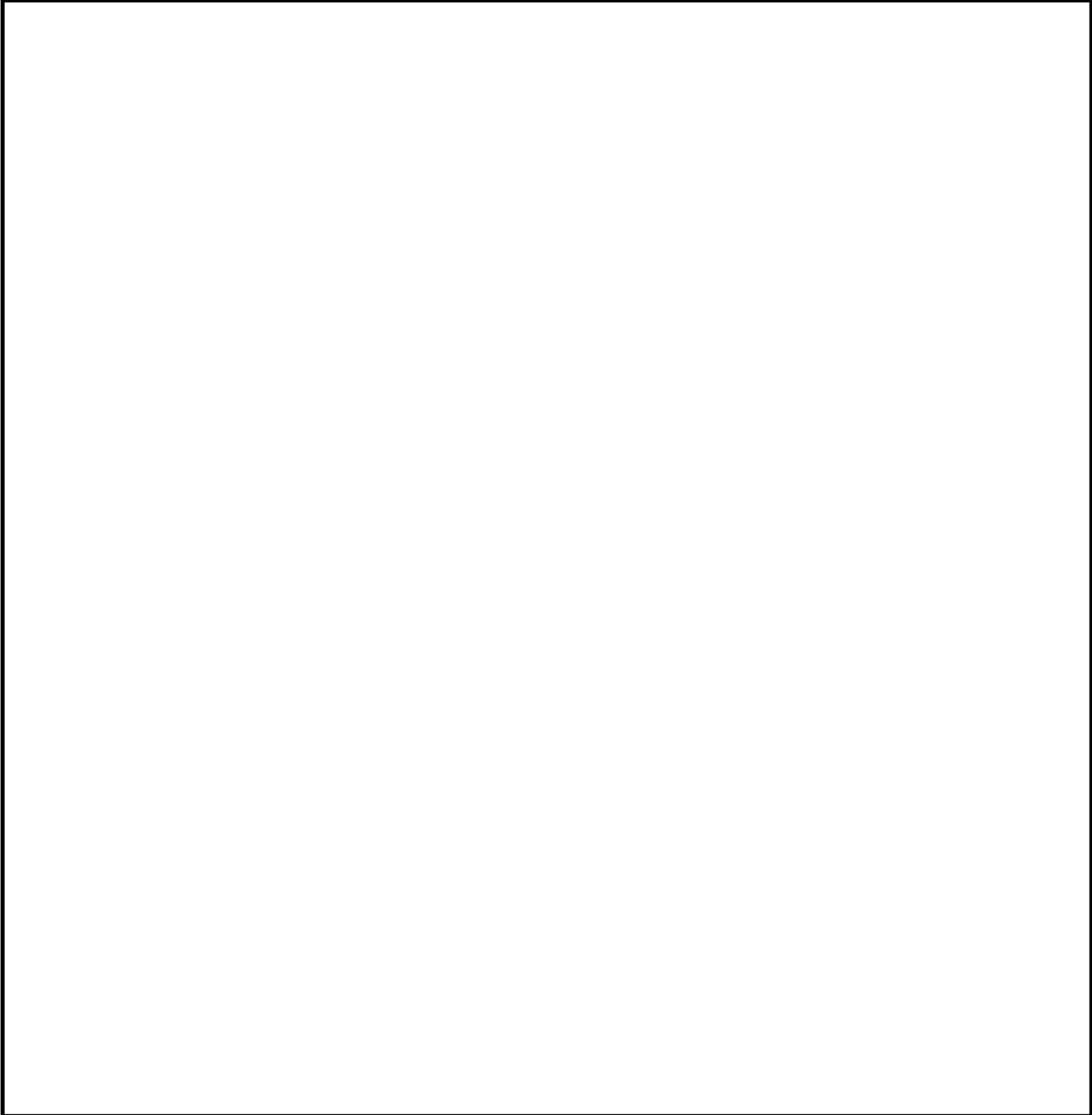


~~TOP SECRET UMBRA~~



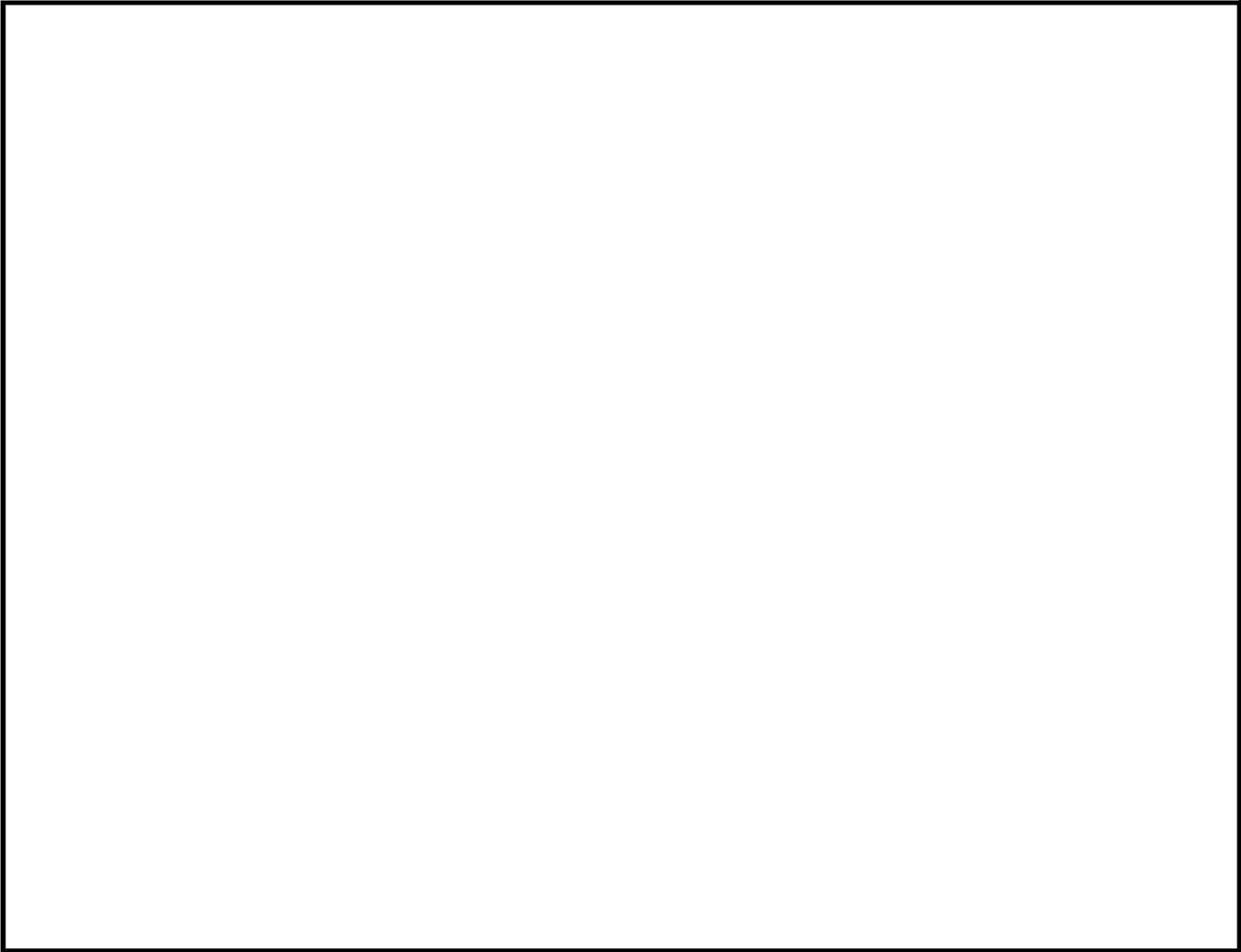
~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605



~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605



~~TOP SECRET UMBRA~~THE REALITY OF COMMUNICATIONS CHANGES

by E. E. Orr, B41

All analysts and managers of analytic efforts must constantly face both the possibility of a communications change on their targets and the consequences of such a change. The term "communications change" frequently causes unnecessary apprehension--the change does not inevitably signal adverse consequences on target identification, maintenance of continuity, and production of SIGINT. Many changes (introduction of new callsigns, frequencies, etc.) on most targets are routine; they occur regularly and are only slight hindrances to the proficient analyst. On the other hand, some communications changes are not routine and do have an adverse effect on SIGINT production. They can result in reduction, or even total loss, of capability to identify and maintain continuity on target communications nets and the specific associated terminals. The latter type of communications change is the subject of this article.

\* \* \* \* \*

Changes which might affect exploitation capability will vary greatly for different targets, depending on the extent of current exploitation and on the complexity of the newly introduced operational procedures. However, knowledge of the relationship between various communications features can greatly assist in prediction of future operational usage. Some features which should be considered follow.

1. SOI life expectancy: Most signal officers are systematic in their Signal Operating Instructions (SOI) and are apt to practice cyclic introduction of new materials such as callsign systems. Knowledge of their idiosyncrasies helps in predicting the extent and date of a change. In any event, operating materials which have been in use for extremely long periods are more likely to be replaced than those recently introduced.

2. Cryptographic continuity: Past experience shows that a change in such operational communications procedures as callsign or frequency usage is not usually accompanied by a change in the cryptographic procedures applied to either valid or non-valid text--probably because different organizations and personnel are involved. Usually, the cryptographer does not

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

transmit the message, and the transmitting operator is not aware of the method of encryption. Thus, textual characteristics can often be exploited in lieu of external characteristics and vice versa.

3. Sudden versus gradual change: Many changes (e.g., newly allocated frequencies) can be implemented immediately upon receipt. Other changes require "live" testing and extensive operator training and orientation. The following changes, for example, would probably require an extended period for implementation:

a. Introduction of a more sophisticated mode of communications: Equipment procurement is usually limited, and testing and training are required before the new system becomes operational.

b. Use of a new Morse cut number system: Operator training is obviously required prior to full implementation.

c. Introduction of

is an example of a change requiring extensive operator training.

Some indicators of an impending communications change are:

1. Temporary extension of the normal period of use of existing SOI materials.

2. Limited testing of new procedures on existing links/nets or on supplementary communications.

3. Direct references in chatter to new procedures. Such references could consist of anything from a casual implication to a statement of the effective date and type of new SOI materials.

4. Trends toward standardization or diversification, whichever is applicable.

5. Use of, or references, to, more sophisticated modes of communication.

\* \* \* \* \*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Although the ability to predict impending communications changes is a distinct advantage, recovery of continuity on target communications is greatly expedited by contingency planning which defines actions to be taken following introduction of new SOI materials. Contingency planning in preparation for subsequent analytic recovery must be realistic and flexible. Consideration should be given to the following factors:

1. Timely field station reporting of deviations from the norm: As the mission of most collection sites is limited in scope, this reporting permits higher echelon to make an early assessment of the overall extent of the communications change, to advise all elements concerned, and to issue necessary instructions.
2. Target recognition/identification: Even though such things as callsign and frequency usage have changed, the best source of target recognition/identification is the operator who has copied the target in the past and who will probably recognize it in the future. Operator identifications should be considered valid unless disproved. These identifications should be provided, in a format usable for traffic identification, to other field sites which are tasked with similar targets and which are likewise encountering difficulty in isolation and identification of mission targets. Thus, time will not be wasted in copying communications which are another site's mission.
3. Establishing procedures for early continuous follow-up collection on potentially mission-associated communications: Although these communications may not be identified beyond nationality, establishing procedures for early collection will prove most advantageous.
4. Determining possible methods of attack as a means of associating homogeneous intercept and performing follow-on analysis: In making this determination, we must ask, "What would we do if the old tried and proven analytic techniques and aids were no longer available?" A definitive answer to this question will probably not be found, but alternate approaches can be devised. For example, if callsigns cannot be exploited, related intercept can often be associated on the basis of cryptographic features. These features may, therefore, need examination very early after a communications change.

~~TOP SECRET UMBRA~~

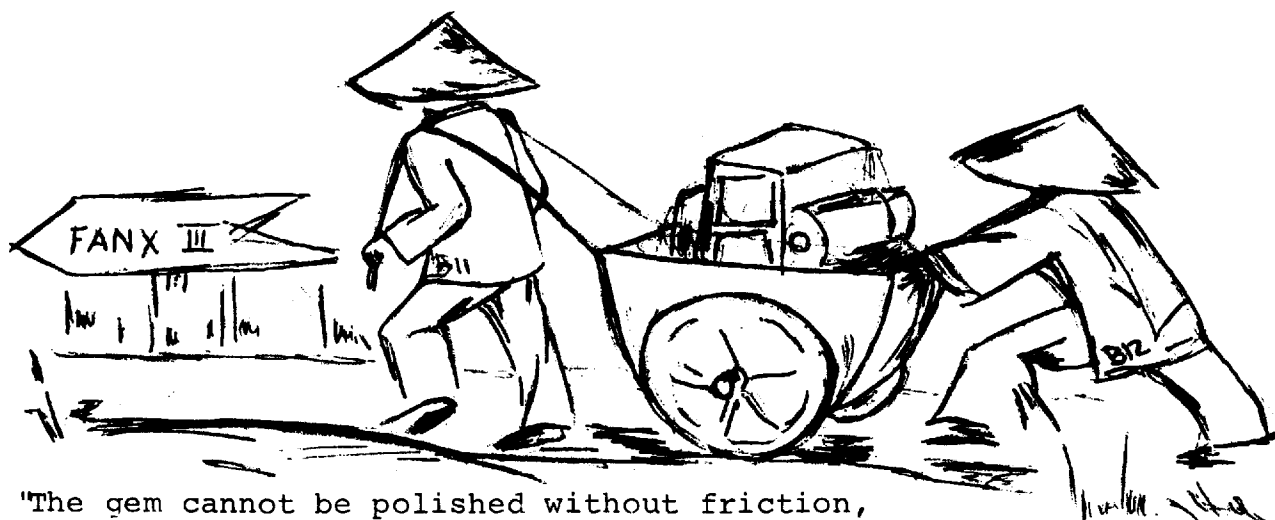
~~TOP SECRET UMBRA~~

5. Once the possible methods of attack have been determined, developing detailed procedures for quick implementation: These procedures include issuing instructions to be followed in the event of a communications change, outlining processing (preferably in conjunction with a flow chart), and devising the machine software which would be needed for machine processing. Processing of data after an extensive communications change does not require completely new procedures, although some alteration or expansion of existing standard procedures will probably be necessary. Maximum retention of established procedures, which are already well known to all operating elements, will cause minimum confusion following a communications change and will aid in early recovery.

6. Maintaining continuous documentation on all special processing or analytic actions taken and the type, extent, and data of actual changes in target SOI: This documentation will aid in keeping all elements currently informed and in preparing for later SOI changes.

\* \* \* \* \*

If this article succeeds in stimulating more realistic planning for future communications changes, deterioration of SIGINT production after such changes will be minimal.



"The gem cannot be polished without friction,  
nor man perfected without trials."

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~A NEED FOR A CENTRALIZED TRANSCRIPTION OPERATION

by Richard S. Chun, B44

It is well known that the introduction of new and more sophisticated voice communications facilities by B target countries is expected to produce a corresponding increase in the volume of voice intercept. It is also well known that the shortage of transcribers, both in the field and at NSA, will become increasingly critical if we continue the present concept of voice operations.

B's problems are even more exacerbated by the fragmented and diversified voice transcription setup now in effect. Three voice processing laboratories (probably four after the transfer of F441's mission and functions to NSA in June 1972) are managed operationally by the several B operating elements, but the equipment accountability and maintenance is the responsibility of B44. This results in varied and parochial processing and reporting procedures, training doctrines, priorities, and records and files maintenance systems. Further, experienced transcribers assigned to elements which require little transcription work have moved to more lucrative career fields, thus producing the current feast-or-famine transcription resources situation in B.

Most of these problems could be solved by having B's voice transcription operation under a single management at a single location. A centralized voice transcription operation which assembles in one unit the career-minded and professional linguists would help ease the acute shortage of transcribers/linguists, since the experienced linguists can be cross-trained to process any communications entity.

B at present has no documented standards for consolidated voice tape accountability/disposition records, intercept requirements/priorities, RT handbooks, training aids, standardization of terms, training doctrines, or other data necessary for an effective and efficient total voice transcription operation. These requirements can best be met under centralized management. Ten or more steps are presently necessary to process a single multichannel tape from intercept to degaussing (i.e., erasing)--not including the numerous other steps performed by the analysts handling the same tape before it reaches the OPI. A centralized

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

effort would limit these steps to intercept, demuxing, transcription, translation, and forwarding of processed material to the OPI analysts.

Other advantages that would accrue from a centralized B transcription operation follow:

#### OPERATIONS

a. Adjustments can be made to loss of transcribers, changing field transcription capabilities, and shifting requirements.

b. A central control for voice-related technical services (e.g., signal analysis, data processing, etc.), technical support to field operations, coordinating/effecting voice intercept, equipment accountability, maintenance and operational quality control, and for voice-related research and development including special projects.

c. Establishment of standardized voice transcription processing and reporting procedures/formats, a single operational training doctrine including SOT/OJT and intern programs, and a centralized voice-related language research effort.

#### ADMINISTRATIVE AND HUMAN FACTORS

a. Elimination of administrative redundancies under the single management and better long term programming and planning (space, personnel, equipment).

b. More opportunity to increase transcriber language capabilities by offering greater variety of assignments and improve transcriber morale with better career planning (professionalization).

\* \* \* \*

~~TOP SECRET UMBRA~~





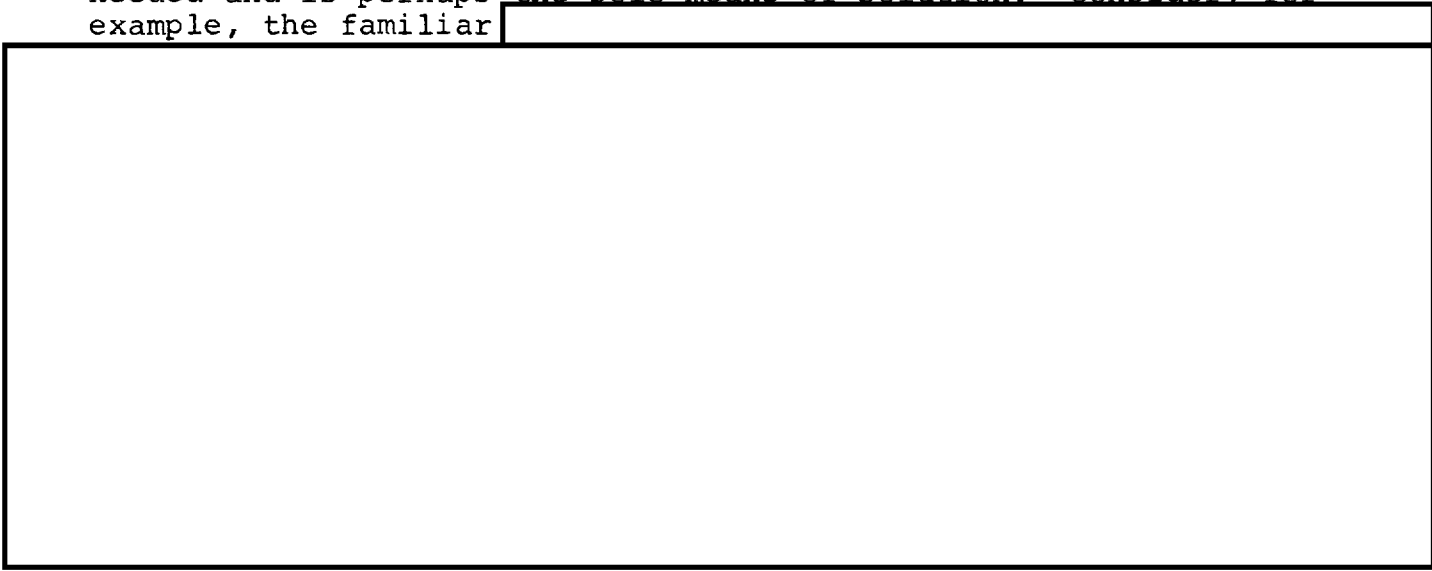
### THE OPEN DOOR

We seek to be companions along the way.  
The lantern which we carry is not ours.  
The spirit which we share is contagious thought;  
The knowledge which we gain, an illuminating  
torch  
And all who seek may perceive and learn.

-The Concept of Dragon Seeds

THE ROLE OF MATHEMATICS IN C/A  
by Dr. Ralph W. Jollensten, P1

There are often cases in cryptanalysis where mathematics is needed and is perhaps the sole means of solution. Consider, for example, the familiar



These examples should make it apparent to all that the degree to which mathematics can be used in cryptanalysis depends upon at least three factors: (1) the nature of the C/A problem,

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

(2) the mathematical background of the analyst, and (3) the imagination and cleverness with which the analyst can apply his background knowledge to the problem.

Perhaps the most important factor is "the imagination and cleverness with which the analyst can apply his mathematical knowledge to the problem." Analysts often look at a C/A problem and conclude that mathematics is not applicable to the case. Mathematicians are often hired to fill C/A intern billets and soon bemoan the lack of opportunity to apply their skills. C/A interns take probability and statistics courses programmed by the C/A Panel, and upon completion are asked, "To what extent does the course apply to your job?" In many cases, the answer is, "Not at all." I believe that in these situations the main reason the analyst cannot see an opportunity to apply mathematics to C/A, is a lack of imagination or desire rather than a lack of experience.

Non-mathematicians are frequently stymied by mathematical symbols and notations, and hence shy away from its use; while mathematicians who may be inexperienced in cryptanalysis often attempt to apply their skill 100% of the time, whether or not it is required.

It is often difficult for an analyst to compile a mathematical formulation applicable to any problem, much less a cryptanalytic one. Imagination, intuition, and patience are required in formulating mathematical problems. One should not expect to become an efficient practicing mathematician overnight.

My advice to the young mathematician who bemoans the fact that he cannot apply his trade as much as he would like is this:

1. Don't try to apply mathematics to every phase of the problem--an all-encompassing approach is often impractical. Look for opportunities to apply different facets of the subject to different phases, bits, and pieces of the problem. For example, use counting techniques to compute work factors to see if a particular method will work in a practicable amount of time; use

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

statistics to set thresholds; use euclidian n-spaces as models in which to imbed frequency counts; use probability to compute the odds in favor of one hypothesis over another.

2. Don't insist on using only your particular specialty--algebra, analysis, or whatever it might be. Be willing to look for opportunities to apply other facets of mathematics.

3. Read the literature available in our libraries on the application of various branches of mathematics to C/A. Become acquainted with specific cases which demonstrate the wide and deep applications of mathematics such as PTAH, eigenvector techniques, Fourier analysis, and applications of polynomials over a mod 2 field.

My advice to non-mathematicians is this:

1. Don't shy away from mathematics because you don't understand it. If you are thoroughly familiar with the crypt-analytic principles involved, the problem itself will help you to understand why certain mathematical techniques work.

2. Don't let symbols and notations throw you; use your cryptanalytic ability to "break" the plain code used in the mathematical world.

3. Make an effort to improve your understanding of the subject. Especially concentrate on understanding probability and statistics and attempt to associate mathematical models to crypt-analytic problems.

A student once asked me why he should study the effects of rolling a die, since we didn't run into dice in cryptanalysis. I said, "In your homework, which would you rather consider? Rolling a die with six sides or a die with 26 sides?" The probability of seeing an A or any other letter from B through Z in "flat random" cipher would be  $1/26$ , and a die of 26 sides is a reasonable model. But the student could not see beyond the surface.

Finally, for all analysts, keep an open mind about the use of mathematics in C/A; and remember, opportunities to use new mathematical techniques in C/A creep up when you least expect them.

~~TOP SECRET UMBRA~~

CRYPTO-SCRAMBLE

Richard Atkinson

Unscramble each of the five numbered crypto-scrambles, placing one letter in each space, to form five words or names, each of which fits the definition to its right.

1. M A N F R E D A S Q U I R E  
\_ \_ \_ O \_ \_ \_ Q Q \_ \_ \_

Rotor development table (2 wds).

2. R A H R I C H E Y  
\_ O \_ O \_ \_ \_

Order of superiority in a set of wheels driven by notch rings.

3. A L L P A L E R  
\_ \_ O \_ \_ O \_ \_

Pair of wires of equal length.

4. N O F I T I T O N A C A R  
\_ \_ \_ O \_ \_ \_ \_ \_ O

Encipherment process involving encipherment, disassociation, and further encipherment.

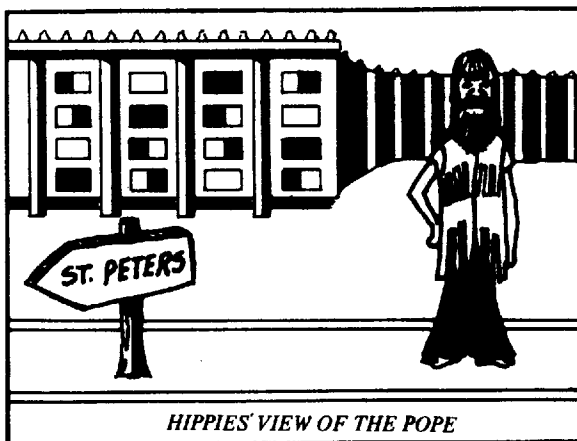
5. D E A L S P E N T  
\_ \_ \_ \_ O \_ \_ O

Stationary sets of contacts at the end of a maze.

Now arrange the circled letters to form the cryptoanswer suggested by the cartoon at the right.

Print CRYPTOANSWER here

-----



Answer on page 31

~~TOP SECRET UMBRA~~MACHINE-AIDED TRANSLATION

by Norman Wild, B03

Machine translation has been disappointing to optimists, but its failure to measure up to acceptable human standards should not lead us to dismiss "the whole thing" as a total loss. If the machine cannot turn out good translations, it can provide welcome help to human translators. In this and in two subsequent articles, Mr. Wild discusses the problems inherent in translation, the use of machines to aid translation, and the history of such use in NSA.

Problems of Translation

In considering translation, two classes of problems are evident: those which are fundamental and which would exist whether the translator is a man or a machine; and those which, while they are of lesser magnitude, still create difficulty especially for any machine-aided translation.

The fundamental problems are two:

1. Language texts are often ambiguous; they are open to more than one translation into the target language. By this I mean translations which differ in substance, not merely in stylistic choices. Many of these ambiguities are resolved by knowledge of the real world rather than by mechanical examination of immediate context. The human translator can usually tell whether *xiang* means "elephant" or "photograph," or whether *chinsen* means "wages" or "sunken ship." If he is translating English into Russian, he should know which of three Russian words to use to translate "Poles riot in Gdansk," "Lineman injured in fall off pole," or "To the pole with Peary." It is hard to imagine a finite program that would put all the necessary background information into a machine.

2. Languages do not correspond one-to-one. A word or phrase in the original language has some fit with a word or phrase in the target language, but they do not match exactly. The translator has to decide which word to choose

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

when none is exactly right and several are partially right, what to omit because it cannot be carried over into the target language, and what to supply even if the original language did not indicate it. For example, the original language may have omitted the subject and tense of the verb, which are necessary for an English sentence. The translator is not looking for the one right answer but for the closest answer, and different answers may be used for different purposes. Such choices are difficult to leave to a machine program--but perhaps not impossible.

Some lesser problems create difficulties especially for machine-aided translation.

1. The original text must be typed or key-punched with a very high degree of accuracy. The machine does not correct errors as readily as the human being. If the text is not in Roman or Cyrillic, or if it has special characters, a cumbersome arbitrary coding may be necessary. In extreme cases, a satisfactory input may take more time and require a rarer skill than the translation itself. Of course, it helps a lot if the text is already in machinable form for other reasons.

2. The target language may have highly inconsistent usage. Consider, for example, the English usage *in* Ireland, *on* Cyprus, and *at* home for the same locative meaning. Unidiomatic choices by the machine can add an element of confusion or at least of unfamiliarity which slows down comprehension. Feeding all usage in would make for a very cumbersome program.

3. Finding the base form requires a great deal of analysis and programming or a large, burdensome vocabulary list. If the program is not designed to isolate and identify the base form--roughly speaking, the form under which a word is listed in a dictionary--all possible variations have to be stored. Consider two numbers, three genders, and six cases of Russian nouns. Even then, finding the inflection at the end of a Russian word (and allowing for ambiguities and irregularities) is easier than finding the base form in a language which modifies the base in other ways; e.g., *niliijumiza*, "I hurt myself," from *-umia*, "to be hurt."

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

4. The unit of translation may not be neatly set off by white space. It may be part of an unbroken stream of syllables or even of letters from which it must be extracted, and there may be more than one way to divide the stream.

5. The unit of translation may be disconnected as in *er brachte xxx um*, "he killed xxx," and *weile xxx qijian*, "for the purpose of xxx," "what did you xxx for?", or "why did you xxx?" The translator must hold the first element in memory until the second element is found. The second element may come much later; it may not come at all (in which case the left-hand element has a different meaning); or when it does come, it may be coincidental and not belong with the first element. People handle this situation better than machines.

6. The contextual clue may be far separated from the ambiguous word rather than immediately adjacent. For example, a man's name may be spelled in full at first mention in a Japanese text, and thereafter throughout the text, or even in other texts at a later date, the name will be given in a drastically abbreviated form.

7. People respond better than machines to nonce-words or nonce-usages. These are words or usages which never existed before but have been coined for an immediate purpose. For example, any foreign word or proper name could conceivably occur in a Japanese text, when appropriate, in a distorted form. The translator who sees *aparutohaito* for the first time in a context dealing with South Africa should have no trouble reading it as "apartheid." He should not even be bothered much by *hanpatsu* (literally "repulsion") as "backlash" in a Japanese discussion of the American election campaign of 1964. A finite program could not predict all possibilities and enter them in advance. New meanings for old words must be caught semantically from the context, or at least, it must be realized that the old meaning does not hold. Machine translation presents a special problem when a closed group of correspondents, who share a context, use abbreviated or distorted language which is clear to them but baffling to outsiders.

Vocabularies, whether general or technical, are larger than people realize. The suggestion of a micro-glossary, to contain only those words which will occur in the text to be translated, brings to mind "If I knew where I was going to die, I wouldn't go near there."

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

A more modest goal than machine translation is automatic look-up. In this operation, the machine program finds words (or units of look-up) in the text, finds the target-language meaning on a dictionary tape, and prints the meaning. Automatic look-up saves a lot of time, but it could be a dangerous tool for the translator. In the next article, we will look at some of the pros and cons for the use of automatic look-up.

\*\*\*\*

ODE TO A VIETNAMESE CRYPPIE

Minnie M. Kenny, B03

Last night as I drifted to sleep,  
A word to my conscious did creep.  
All night it stayed with me; it just wouldn't leave.  
The word, my dear Dunc, was *receive*.

To work in the morn I did fly.  
On my worksheet a pattern I spied.  
I'm excited, delighted, relieved.  
The word, my dear Dunc, was *receive*.

So, little by little it's read.  
The wheels spin around in my head.  
Next comes *for*. Look! Here's *from*. (Oh! what glee!)  
Why, yes. There's the word *Tri-Party*.

Now put up your pencil, my dear.  
(The matrix's too long to put here.)  
Don't worry or fret. The next one you'll get.  
The language? Cambodian, I fear.

~~TOP SECRET UMBRA~~



EO 3.3b(3)  
PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~

STUDY OF ZFK MESSAGE ACTIVITY, CHICOM [REDACTED]

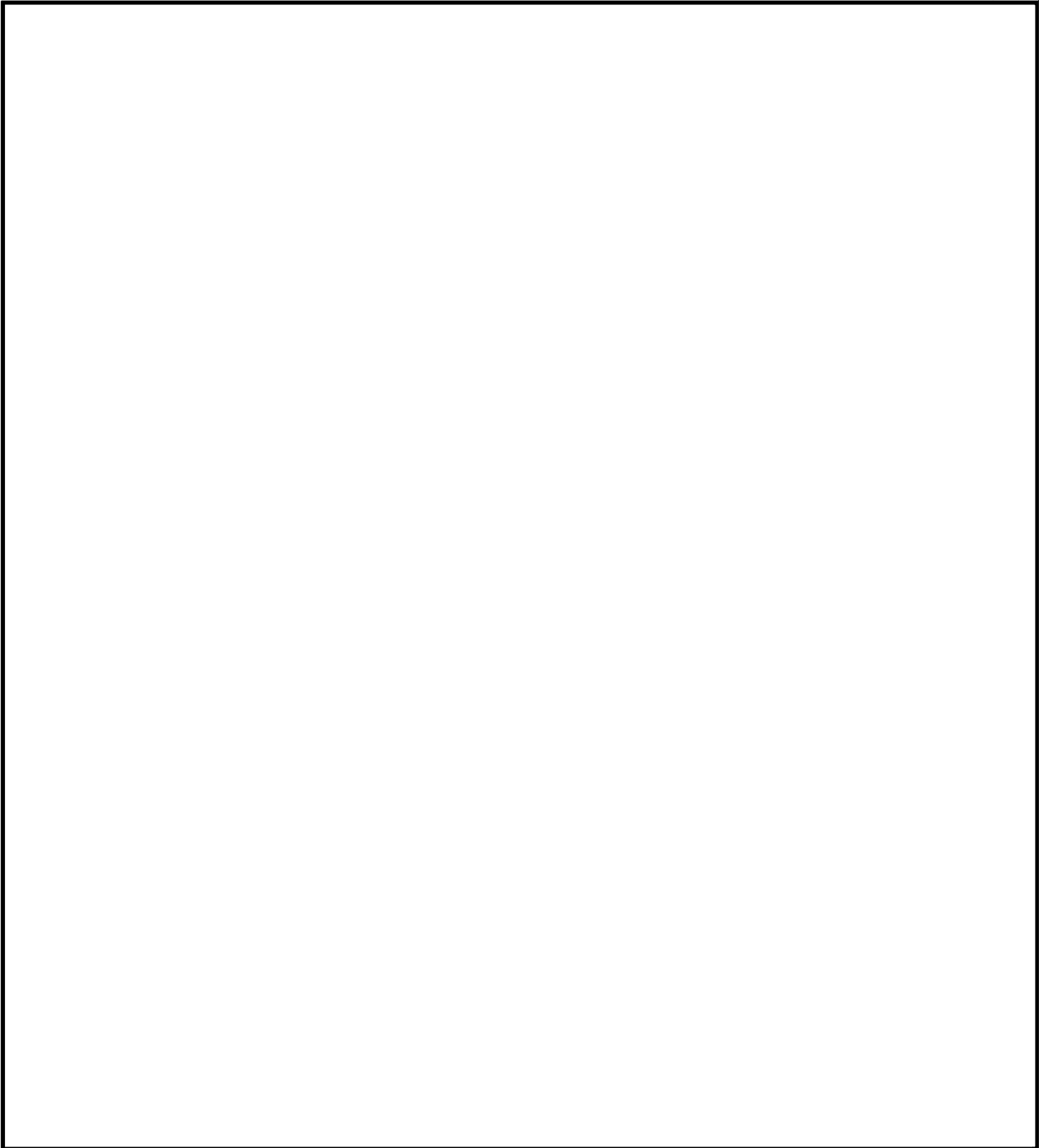
by Kenneth Miller, B433



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

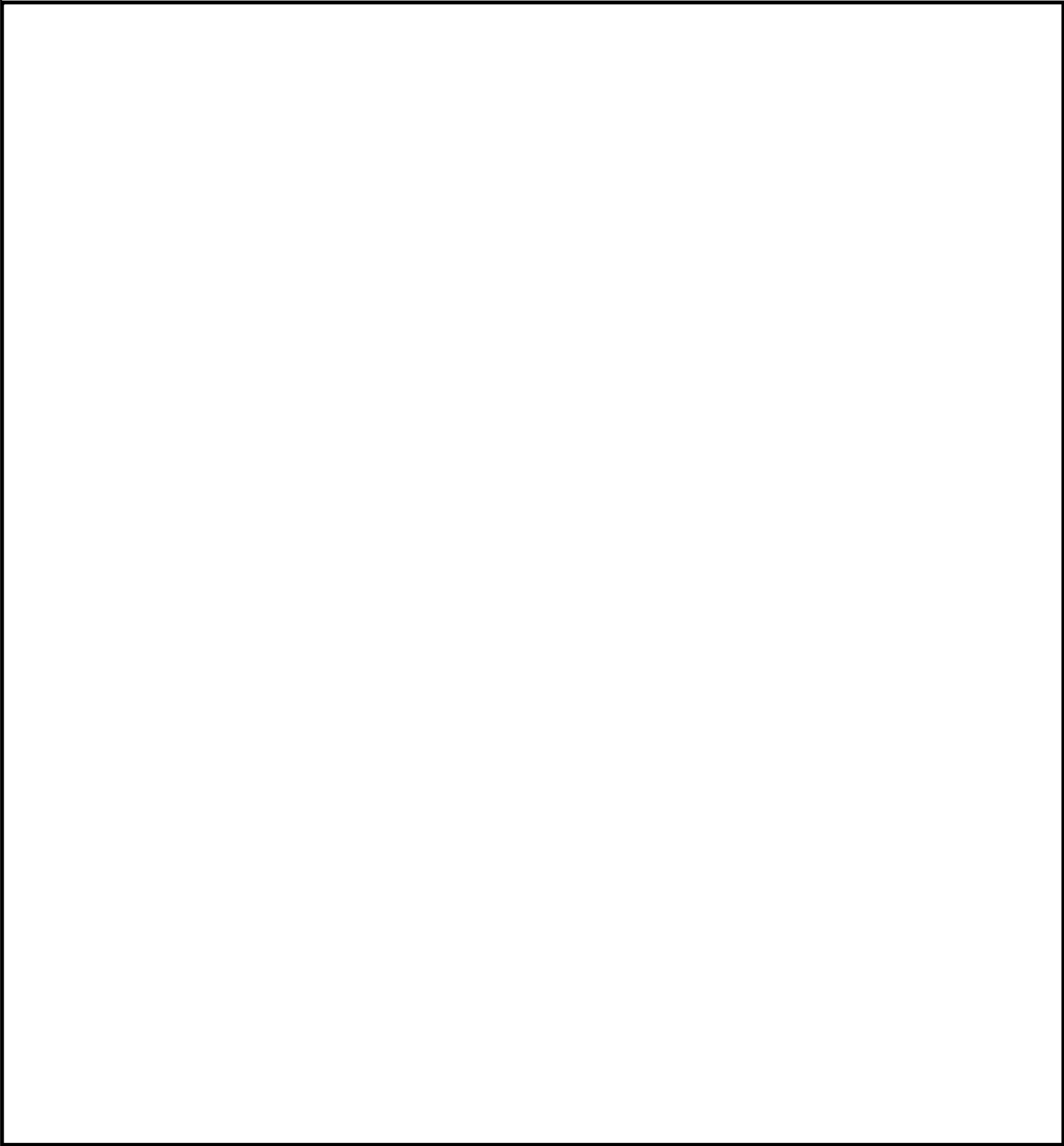


~~TOP SECRET UMBRA~~

Doc

EO 3.3p(3)  
ID: 6708418  
PL 86-36/50 USC 3605

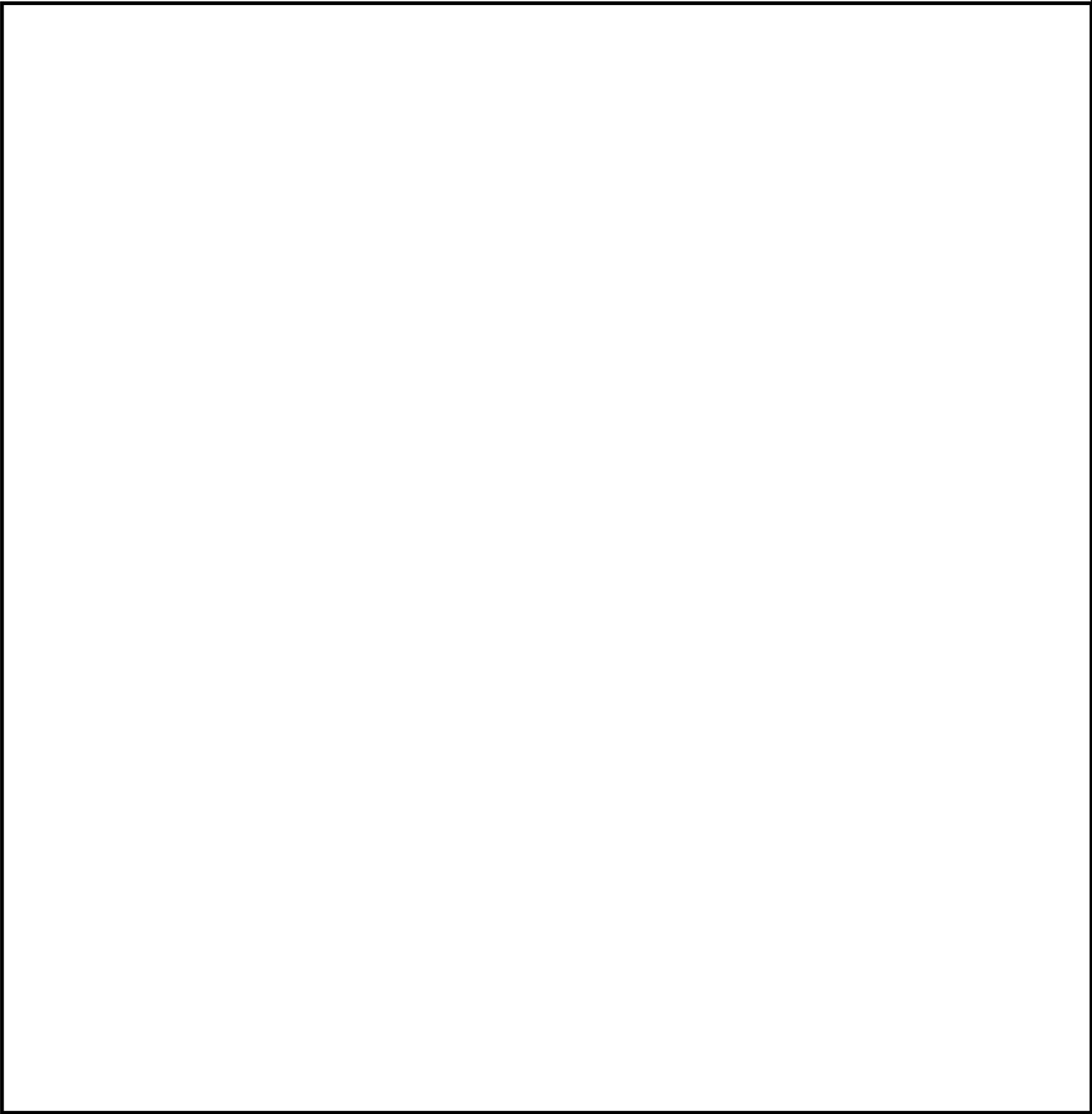
~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

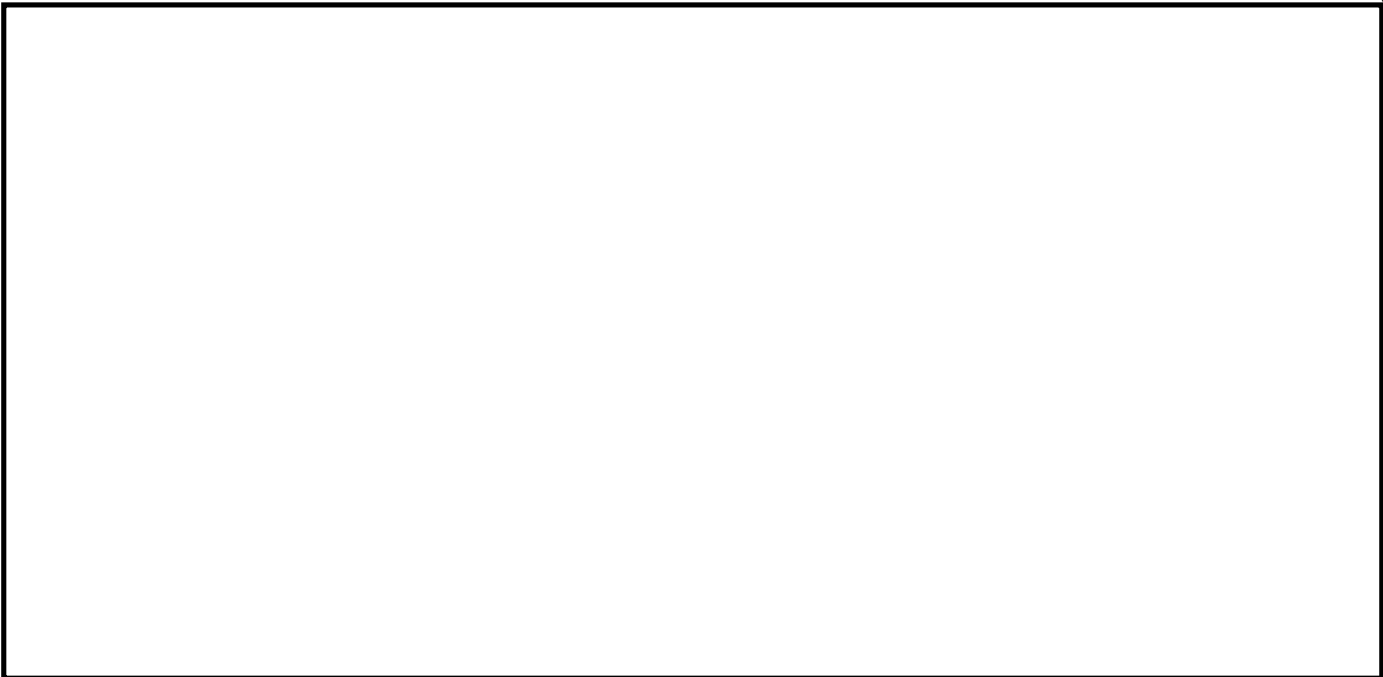
EO 3.3b(3)  
PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



\*\*\*\*

ANSWERS

Answer to Crypto-Scramble

- 1. Friedman Square
- 2. Hierarchy
- 3. Parallel
- 4. Fractionation
- 5. Endplate

Cryptoanswer: Latin Square

Answer to puzzle sent to the Dragon Lady

- 1. .../.../.../.../.../.../... = SISSIES
- 2. -/---/---/---/---/--- = TOMTOM
- 3. -/..-/..-/..-/..-/.. = TARTAR

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

VIETNAMESE COMMUNIST TACTICAL COMINT OPERATIONS ~~(SECRET)~~  
by Tim Murphy, B6

The Vietnamese Communist COMINT effort in South Vietnam is quite extensive but very much decentralized. Its purpose is simply to gather and disseminate tactical intelligence on a timely basis to Communist units in the field. In short, the enemy's COMINT elements function in much the same way as U.S. and Allied direct support units do. Their COMINT units are usually organic to fronts, divisions, or equivalent organizations and all tasking, processing, and reporting appear to be done at that or a lower echelon. The Communists have no NSA-type organization in South Vietnam.

Vietnamese Communist COMINT units are generally comprised of a number of mobile intercept teams and an element which has responsibility for processing and reporting the collected information. Often these intercept teams are attached to units on combat missions in order to provide direct support. They are tasked by the Intelligence Section of the parent organization's Military Staff through the COMINT unit's headquarters.

Typical of Vietnamese Communist COMINT organizations is Front 4's COMINT Unit 508. This independent military intelligence unit, which is directly subordinate to the Front Headquarters, operates in Quang Nam Province of South Vietnam. Our own exploitation of Communist communications has disclosed that COMINT Unit 508 conducts an extensive radio intercept, processing, and reporting effort against U.S., South Vietnamese, and South Korean communications.

COMINT Unit 508 has been remarkably successful in exploiting Allied tactical communications. Intelligence information frequently reported falls into several categories such as the disposition of Allied forces, requests for support (e.g., air, artillery, medevac), Allied after-action reports, Allied intelligence activities, future plans, and VIP activity. Their reports are quite timely and have contained information transmitted by the Allies slightly more than an hour earlier.

The mode of operation is for the intercept team to forward the collected data to COMINT Unit 508's processing element (Team 1). There, detailed intelligence summaries--in many

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

respects similar to the daily summaries issued by U.S. collection sites in Vietnam--are prepared and forwarded. A typical summary was passed on

Like other Vietnamese Communist intercept teams, COMINT Unit 508's teams concentrate their efforts against targets which are most easily exploited (i.e., Allied plaintext tactical voice communications). In addition, they intercept and exploit some ARVN encrypted communications. The processing element provides technical support to the intercept teams via aperiodic technical messages. These messages typically contain data on Allied callsigns, frequencies, and crypt system recoveries. Intercept teams are at times requested to aid in recovering frequencies of various Allied units.

Vietnamese Communist COMINT units apparently do not have organic communications, but rather share the communications facilities of their parent command. Generally, landline telephones or couriers are used for passing COMINT reports, but both COMINT Unit 508 and the Long An Subregion's COMINT unit west of Saigon use radiotelephones extensively. As a result, details concerning the composition and modus operandi of their COMINT organizations are available.

\*\*\*\*

*"Of the 36 ways to fight, the best is to flee."  
Old Chinese Proverb*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

----What with the reorganization of B6 and the relocation at FANX of B1, you are reminded to update your organizational telephone directories to reflect related changes. Also about calls to FANX, don't be discouraged if you are disconnected "amid streams." Just hang up and call again. It seems that the modern convenience of efficient communications links has not reached that new-world outpost yet. (A bit ironic, considering the business we're in?)

\*\*\*\*

----The establishment of the Cryptologic Education Fellowship Program was announced in a memorandum from the Commandant of the National Cryptologic School dated 17 December 1971. The program is open to civilian and military employees with a broad background in cryptology or related technical fields. Those selected will be assigned to the NCSch for a year to participate in the development of training programs and in teaching, with

educational opportunities in fields related to their assignments available as well. Typical assignments for fellowship study are identified for area specialists, cryptanalysts, electrical engineers, computer scientists, mathematicians, cryptologists, and historians.

Applications should be submitted through supervisory channels. Questions on the program will be answered by Mr. Walter P. Sharp (8051 or 796-6334).  
(SECRET)

\*\*\*\*

EO 3.3b(3)  
PL 86-36/50 USC 3605

----There has been quite a bit of interest in B1203's Project BABEL since Carol Leve, P26, touched briefly on its concept and included

[redacted] portion in her speech before the Bookbreakers Forum in April. Using the Stromberg-Carlson 4060 Plotter, B1203 has [redacted]

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

in an effort to furnish the

A discussion of the techniques used will appear as an article in the next issue of *Dragon Seeds*.

\*\*\*\*

----The National Cryptologic School now offers a course in the diagnosis of manual cryptosystems as part of the cryptanalysis curriculum. Designed to be taken after completion of General Cryptanalysis CA-100, which stresses cryptography and exploitation of known cryptosystems, Practical Diagnosis CA-260 teaches the diagnosis of unknown cryptosystems.

Diagnosis is presented as a 5-step iterative process: gathering the a priori information, separating the undifferentiated traffic into homogeneous sets, analyzing the sets and making hypotheses, testing and proving the hypotheses and writing a solution report. A popular feature of the course is that the student acquires his skills by diagnosing a variety of operational foreign language problems from A, B, and G Groups. Statistical and computer techniques are emphasized.

This course is scheduled to be given only once in FY73, from 18 Sep-17 Nov. Successful completion of CA-100 and an entrance exam are required.

\*\*\*\*

----P16 has as part of its mission to maintain an awareness of the state of language work throughout PROD. It is thus required to know such things as the quality of language work performed by PROD linguists, their need for working aids, machine aids, training, and so forth. Frequently P16 can provide or assist in providing such aids and, at times, to train linguists. Several persons in P16 are deeply engaged in machine programs whose aim is to assist operational linguists in their daily work. Staff linguists versed in Cambodian, Vietnamese, Burmese, Thai, and Chinese can be made available to operational elements to assist with special projects or with language problems during periods of unusually heavy activity. For more information contact Mr. Lawrence, Chief, P16, ext 3957.

\*\*\*\*

----Have you ever wondered how to apply machine techniques to traffic analysis? This very subject is treated quite interestingly in a course offered by the National Cryptologic School. TA-261, Computer Aid to Traffic Analysis, introduces the student to various machine techniques and through practical exercises, shows him how to use numerous machine outputs which aid in analysis. Successful completion of TA-200 and MP-060 (or equivalent courses) are prerequisites.

\*\*\*\*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

ASK  
THE  
DRAGON  
LADY

Dear Dragon Lady:

I have just, very belatedly, got around to reading your Dragon Seeds - undated, but the first and only issue, I believe. I especially liked the charming Foreword signed "The Editors." Printing format was attractive, and limitation of articles to 2 or 3 pages tempted the reader into tackling even unfamiliar subjects. I had a few other reactions I thought I might express for better or for worse.

1. Cryptanalysis Through Functional Linguistics by  
D. P. Lenahan, B222

Interesting even to a non-Vietnamese linguist. Two questions come to mind: What attention is paid to frequency in this analysis? It would seem that the tones would betray themselves by being of much higher frequency than anything else. Are there variants for the tones? If so, this fact, of course could partially conceal the disparity in frequencies, but there are good ways to identify the variants. By the way, is Janet King Wild's excellent account of Vietnamese Book-breaking still being read? It dates from the early 1950's, but it is a thoughtful analysis by a brilliant, articulate linguist, and much in it will always be valid.

2. Recovery of a Vietnamese Communist Callsign System  
by Wayne Stoffel, B03

His stress on "the value of historical research" is good and much needed. The tendency to stop work on a superseded system before it is fully understood and to switch to the new system where there is less material available for analysis leads to much waste and frustration. This can be seen in the case of code and cipher systems as well as in callsign analysis. Historical continuity is vital to efficiency and, in many cases, even to the possibility of success. Previous systems must be well documented and available to the analyst. Furthermore,

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

the latter should be required to familiarize himself with the past before being allowed to tackle a new problem.

3. Chinese Voice: Solution to a Dilemma by L. St. Clair Myers, B441

The problem of limited language skill in field voice transcriber/interpreters is a general one. Even outside the Chinese voice area, we accept "the risk of erroneous field translations" much too trustfully. I believe this whole problem needs a good deal more attention with a view to some general solutions.

4. The Creative Translator by Thom Glenn, B61

An excellent article, well expressed

5. Analyzation of Data by Richard Curtin, B11

What's the matter with that quaint old-fashioned word "analysis"? I choked on "initialization", too, midway through the text. Style and sentence structure leave much to be desired. Some parts are downright unintelligible (e.g. paragraph 5).

6. I liked your publication as a whole.

Kay Swift  
G543

P.S.

Having read-again belated-your Nr. 2, I take back what I said about Dick Curtin - or at least I see some reason for the vague and awkward style. Obviously, I did not analyzate the data!

Most of the articles are beyond my ken - or yen - but I found it useful to stretch the mind a little. Mary D'Imperio's article was beautifully organized, clear, and well phrased, as usual.

Mr. Gilbert's comment on honesty in management evaluation was a fine strong cry in the wilderness. The old World War II evaluation check list (diligence, attention to pertinent detail, speed, accuracy, versatility, initiative, etc.) was at least a help in enabling the manager to point out strengths and weaknesses discreetly. And it served periodically to remind

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

both manager and employee of the desirable qualities on which the evaluation should be based. It was discarded - perhaps because it was too much trouble or became so routinized that it was felt to be meaningless. (On a scale of Excellent - Strong - Good - Fair - Unsatisfactor, one woman was given a Good for Accuracy because she was in fact, very bad. She protested to the highest court available!). Nevertheless, I think we are again in a rut and it wouldn't be a bad idea to dust off the old form - or a modified version of it - and see if we couldn't put a little more meaning into our performance appraisals.

Dear Dragon Lady:

"Who spilled the ink on the code room floor?" On page 25 of issue 2 implies that your readers are familiar with Morse code. "Inconsequential Puzzle" on page 22 implies that you think that your readers have time to figure out puzzles, so may be you'd like to run a short Morse quiz, seeing if your readers can make English words out of the following combinations of dots and dashes? All we've done is leave out the spaces between letters.

- 1) .....
- 2) \_ \_ \_ \_ \_
- 3) \_ . \_ . \_ . \_ . \_ .

Conceivably, longer strings of "patterned" Morse strings could be concocted, but I think these three are interesting enough to hold your ditty-hoppers for awhile.

(Answers on page 31)

Harry G. Rosenbluh  
P16

\*\*\*\*

*"Good judgment comes from experience--usually experience which was the result of poor judgment."*

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
EO 3.3b(6)  
PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~

CONTRIBUTORS

RICHARD S. CHUN, Deputy Chief of B44, is from Hawaii and began his cryptologic experience in 1950 as the first SIGINT Korean linguist in the field. He performed as a translator, book-breaker, and interpreter and also conducted interrogation of North Korean prisoners of war. He reported to NSA in 1953, headed the [redacted] for a year, and was reassigned to Korea and then to ASAPAC in Tokyo, where he worked on [redacted].

[redacted] Following his conversion from a U.S. Army major to civilian in 1962, he first served as the Deputy Chief of B27 (now B11) and later worked on various other PRC and NVN problems here at NSA and at JSPC, where he initiated the first [redacted] communications intercept from ACRP. Mr. Chun's commendations include the Legion of Merit, U.S. Army Commendation Medal, and [redacted] Distinguished Military Service Medal for his SIGINT efforts. He is the designer of several analytic working aids including the "Chun Wheel," which is being used by Air and Air Defense analysts throughout the world, and is a Korean, Chinese Mandarin, and Japanese linguist.

HERB GUY, B403, has spent most of his 20 years of cryptologic service in P1 and B4 or their predecessor organizations. He has a B.A. from the University of Florida and an M.A. from the University of Michigan, both in mathematics. In 1970-71, he attended the Naval War College. Although most of his Agency experience has been in cryptanalysis, he is also certified as a Mathematician and a Special Research Analyst.

DR. RALPH W. JOLLENSTEN received his B.A. in Mathematics from Hastings College (Nebraska), his M.A. in Mathematics and Science from the University of Nebraska, and his PhD in Mathematics from the University of Virginia. He has twenty-one years experience at NSA, where he is currently Deputy Chief of P12. Dr. Jollensten has also served as the Executive of the C/A Career Panel and the head of the Sciences Department of the National Cryptologic School.

EO 3.3(h)(3)  
PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

KEN MILLER, C/A Technician in B4331, has been with NSA since 1965, leaving for a tour with the Marine Corps 1966-1969. On his first assignment, he tackled B41's PRC callsign problem and then moved to B432, the Research Branch of the Cryptologic Research Division. He is currently lending his young talents to the PRC high-grade military, [redacted] problem in B43. The C/A Career Panel has accepted Mr. Miller's article, published in this issue, as fulfillment of a basic requirement for certification as a professional cryptanalyst.

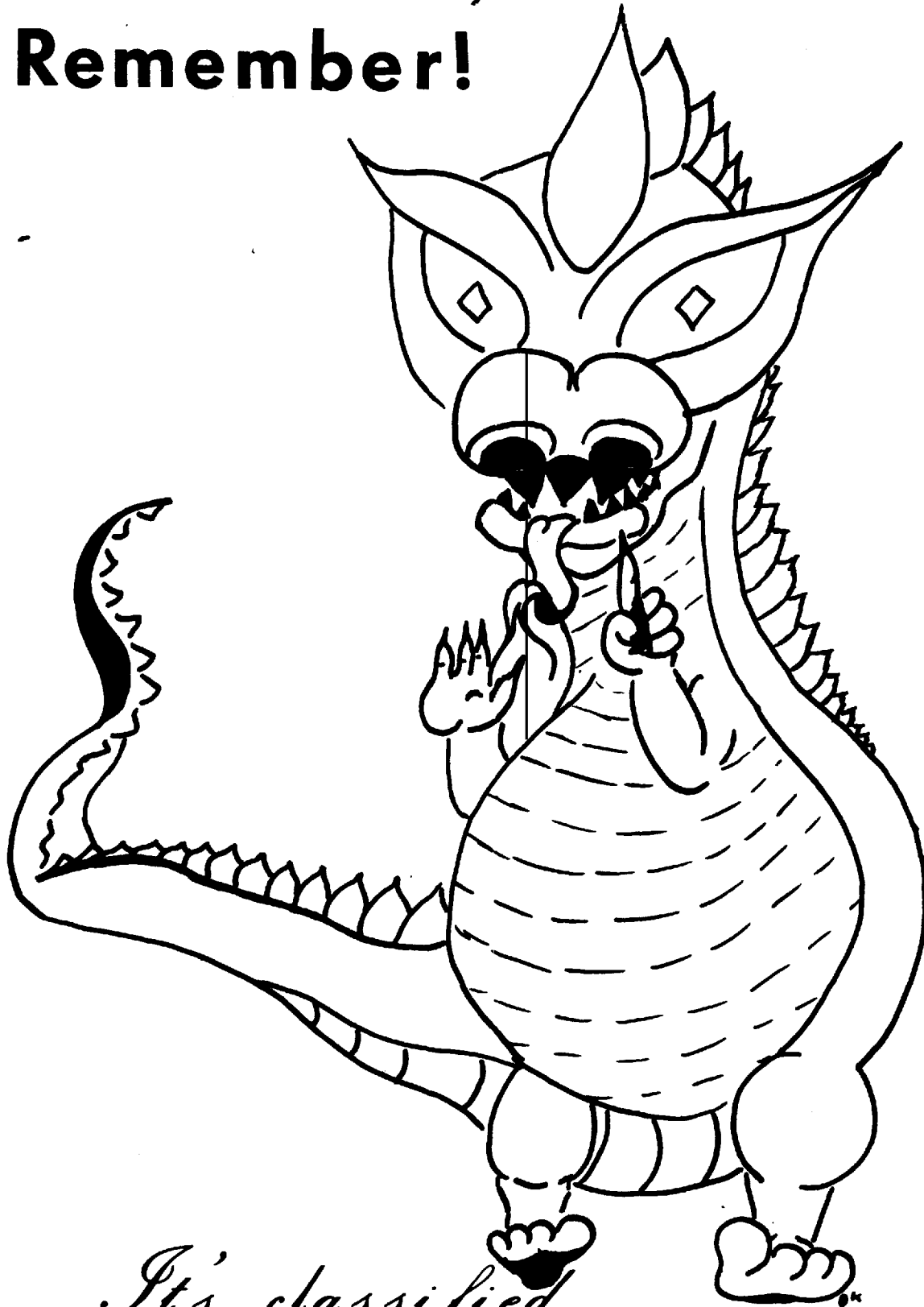
TIM MURPHY, B603, had a wide variety of intelligence experience as an Air Force officer before entering NSA as a civilian in June 1968. He completed the USAFSS Communications Intelligence Officer Course and the CV-100 program before serving with AFSS in Berlin, with Hq 7th Air Force in Saigon, and with Hq, USAF at Fort Meade. From 1968 until his recent assignment to B603, Tim worked as a civilian Traffic Analyst and a Special Research Analyst on the VC Military problem in B62. He received his M.A. in International Relations in 1970 from Georgetown University where, ten years earlier, he had been awarded his B.A. in English.

EUTH E. (ED) ORR, B41, entered the cryptologic world in 1949. His assignments since that time have included Soviet, Chinese Communist, Vietnamese, and Korean problems ranging from [redacted]. He has served in analytic, managerial, staff positions. His close association with PRC development continues in his current assignment as Acting Chief, B41, which is concerned with unidentified PRC communications. Mr. Orr is a graduate of the University of Maryland and holds professional certification in Traffic Analysis and Special Research Analysis.

NORMAL WILD, B03, is one of the Agency's foremost multilinguists. He has been with NSA and predecessor agencies since September 1944, working mainly with Far Eastern languages. (It is reliably reported that he reads STC like plain language.) Mr. Wild's academic background includes the B.A. (1939) and the M.A. in Chinese and Japanese (1941) from Columbia University. He is the author of numerous linguistic reference and training aids within NSA, and has long been concerned with the interplay of computers and language.

~~TOP SECRET UMBRA~~

# Remember!



*It's classified*

~~TOP SECRET~~

**National Security Agency**

Fort George G. Meade, Maryland



**DRAGON SEEDS**

**SEPTEMBER 1972**

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~



~~TOP SECRET UMBRA~~

This is *Dragon Seeds*.

There is fantasy, irony, and the bite of reality in the name. It speaks of the East. And, like the East, it suggests much, says little.

*Dragon Seeds* is both Mother China and her neighbors. *Dragon Seeds* is monumental and minuscule. It is the past and future. It begs for elaboration but gives none. In it are echoed softly slurred Mandarin, brittle Vietnamese, determined Korean. In it is the spectre looming over the Thai, Lao, and Khmer. It is frightening and friendly. It is uncertain.

Above all, *Dragon Seeds* is promise. It is fertile with ideas unbounded, to be cultivated with creativity and imagination. It is challenge. It is alive. It will be more than it is.

*Dragon Seeds* is yours. May it grow with you.

The Editors

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

DRAGON SEEDS

Publisher

DONALD E. MC COWN, CHIEF B03

Managing Editor

Minnie M. Kenny

Feature Editor

Richard V. Curtin

Rewrite Editor

Victor Tanner

Executive Editor

Robert S. Benjamin

Biographical Editor

Jane Dunn

Education Editor

Marian L. Reed

Special Interest Editor

Ray F. Lynch

Composition

Helen Ferrone  
Lorna Selby

PRESS CORPS

B11 Carolyn Y. Brown

B12 Philip J. Gallagher

B21 Gary Stone

B31 Jack Spencer

Thomas M. Beall

B32 Jean Gilligan

B33 Louis Ambrosia

B34 Thomas L. Wood

B41 James W. Schmidt

B42 Peggy Barnhill

B43 Mary Ann Laslo

B44 Jack L. Thomas

B45 John E. Uzarek

B5 Paul M. Hoagberg

B62

B63 George S. Patterson

B63 William Eley

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



Vol. 1  
Nr. 4

September 1972

**TABLE OF CONTENTS**

B Office Chiefs' Biographies		2
Things That Go Clank in the Night	Mike Hricik	7
SIGINT and Automatic Data Processing	Staff	12
SEADEV--Mechanization for T/A Development	Allen L. Gilbert	14
The Open Door: Project KAY-- or Another Kind of RYE	Louise Swanson	17
A Software Approach to Script Processing: The Why	Robert F. Kreinheder	19
A Software Approach to Script Processing: The How	Ferdinand J. Reinke	21
Machine-Aided Translation	Norman Wild	24
Seedlings		27
Ask the Dragon Lady		30
Contributors		32

~~TOP SECRET UMBRA~~

## B OFFICE CHIEFS



DONALD A. REED  
Chief, B1



MICHIE TILLIE  
Chief, B2



COL JOHN E. KENNEDY  
Chief, B3



ROBERT A. HIGHBARGER  
Chief, B4



STEPHEN J. O'TOOLE  
Chief, B5



DONALD C. JACKSON  
Chief, B6

~~TOP SECRET UMBRA~~

"INDEED THE WISE MAN'S OFFICE  
 IS TO WORK BY BEING STILL;  
 HE TEACHES NOT BY SPEECH  
 BUT BY ACCOMPLISHMENT;  
 HE DOES FOR EVERYTHING,  
 NEGLECTING NONE;  
 THEIR LIFE HE GIVES TO ALL,  
 POSSESSING NONE;  
 AND WHAT HE BRINGS TO PASS  
 DEPENDS ON NO ONE ELSE."

- LAO TZU

# 聖人



是以聖人  
 處無為之事  
 行不言之教  
 萬物作焉而不辭  
 生而不有為而不恃  
 功成而弗居  
 夫惟弗居是以不去  
 老子

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

DONALD A. REED  
Chief, B1

In 1948, Air Force Captain Donald A. Reed was one of the first three Air Force officers to be assigned to Arlington Hall from the Russian language school at Monterey. Throughout the remainder of his military career (retired 1 February 1967 in grade of Colonel), he held a variety of key positions in the Air Force Security Service and NSA. These included Operations Officer of the 1st RSM at the time the Korean War broke out; Chief of Analysis Div (OAD) at Hq USAFSS; Chief of the Russian [redacted] problem (242H) from 1952-54; Commander of the 12th RSM at Landsburg and Bingen, Germany; Chief of Operations at the 6901st in Zweibrücken; Director of Operations at Hq USAFSS; Deputy Commander AFSCC at Hq USAFSS; Deputy Commander 6922 Scty Wing at Okinawa; Commander 6925 Scty Gp at Clark AB; and Chief, B2. Upon retirement from the Air Force, Mr. Reed became Chief of B04. For the past year, he has been Chief, B1.

\*\*\*\*

MICHIE F. TILLEY  
Chief, B2

Michie F. Tilley has been with NSA for 19 years. Following World War II service as a Navy radioman, Mr. Tilley worked in private industry and continued his interest in communications as a reserve intercept operator with NSG. He was recalled to active duty during the Korean War, and joined NSA as a communications clerk in 1953. He moved on through Section and Branch Chief jobs in the Indochinese problems to successively more interesting assignments, including Chief, NSAPAC Representative Philippines, and Policy Officer, Hq NSAPAC. In the former capacity he provided the first NSA representation in South Vietnam [redacted] and in the latter was intimately involved in PACOM actions at CINCPAC staff level.

More recently, Mr. Tilley served as Chief, Pacific Branch, Foreign Relations Division (1966/1967), Senior U.S. Liaison Officer, Melbourne (1967-1970), and Deputy Chief, B2 (1971/1972). He has been Chief, B2 since July 1972.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

JOHN E. KENNEDY, COL, USAF  
Chief, B3

The least illustrious of the Boston Kennedys (he claims his relationship to the presidential family is not close enough to do them any harm or him any good), Col Kennedy flew a tour of combat with the 8th Air Force in Europe during World War II. Noteworthy in that stage of his military career is the fact that he was shot down over the Battle of the Bulge and, through compensating navigational errors, he accidentally evaded capture by the Germans. At the end of World War II, he resumed civilian life and founded an only slightly successful business in Massachusetts of which he was a corporate officer.

At the outbreak of the Korean War he was involuntarily recalled to active Air Force duty and flew another combat tour in Korea in a night interdiction fighter-bomber role. Noteworthy in that phase of his military career is the fact that he flew 56 combat missions when only 55 were required. He was responsible for his own record keeping, lost count, and flew the extra mission which almost cost him his life. He was then assigned to Air Force Training Command in Texas, where he taught both air and ground school courses.

Among courses which he wrote and taught were "Memory Improvement" and "Theory of Navigation." During that period of time he completed his formal education at the University of Houston. He then was selected for foreign language training and graduated in 1956, with no honors, from Yale University Institute of Far Eastern Languages.

His cryptologic career began in 1957 with assignment to the National Security Agency. Col Kennedy has filled a number of B3-related positions, both overseas and at Ft Meade since that time. He is generally considered as the pioneer of the concept of cryptologic support to military commands, having established the SSG 7th Air Force, Saigon, and having established and directed the SSG PADAF.

Over the past several years, he has been involved in a number of tactical SIGINT support enterprises, some of which have had a modicum of success. Noteworthy among such efforts

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

was the unsuccessful military operation designed to extract U.S. prisoners of war from the Son Tay prisoner camp in North Vietnam. For his efforts in that operation he was described by WASHINGTON POST columnist Jack Anderson, in a column published in 1971, as a "dubious hero."

His major accomplishments and hobby are his wife, Terry, and his daughter, Mary. He is soon to be involuntarily retired by the Air Force.

\*\*\*\*

ROBERT A. HIGHBARGER  
Chief, B4

Mr. Highbarger joined NSA (AFSA) in June of 1951 after completing his MS in Mathematics at the State University of Iowa. His cryptologic career has been nearly equally divided among P1, ASA, A5, and B Group. He is a certified cryptanalyst who has spent time on the hand and machine ciphers of East Germany, Poland, Russia, North Vietnam, and China.

Since December 1969, Mr. Highbarger has been Chief of B4, which provides technical services to all of B Group.

\*\*\*\*

STEPHEN J. O'TOOLE  
Chief, B5

During World War II, Mr. O'Toole served as a Japanese linguist at Arlington Hall. During the Korean War, he worked as a Korean linguist at Arlington Hall and Hq ASAPAC Tokyo. Between the wars and up until the move to Fort Meade, he was involved in the Soviet problem initially as a linguist and later in supervisory and managerial capacities. When ACOM was formed, he became Chief of the Reporting Staff. Following a year at the Army War College, he became Chief of the CHICOM Exploitation Division. This was followed by assignments as Chief of the Operations Staff of the newly formed B Group and Deputy Chief of the Production Operations and Reporting Staffs. At present, he is Chief B5, the Office of PRC [redacted]

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605DON C. JACKSON  
Chief, B6

Dr. Jackson began his cryptologic career in 1953 as an Ensign in the U.S. Navy, working on the Soviet [redacted] problem at Arlington Hall. He served in various Agency and field positions in a military capacity until 1957, including a tour as Officer-in-Charge of the Naval Security Group Detachment assigned to the Taiwan Defense Command and the U.S. 7th Fleet.

From 1957 to June 1961, he held various Agency assignments including Branch Chief positions for the Chinese Military problems. In July 1961, he became Chief of the Production Organization's resource programming staff, during which time the CCP was born. In 1964, Dr. Jackson was awarded an NSA Fellowship to attend George Washington University, where he completed requirements for the Doctorate degree.

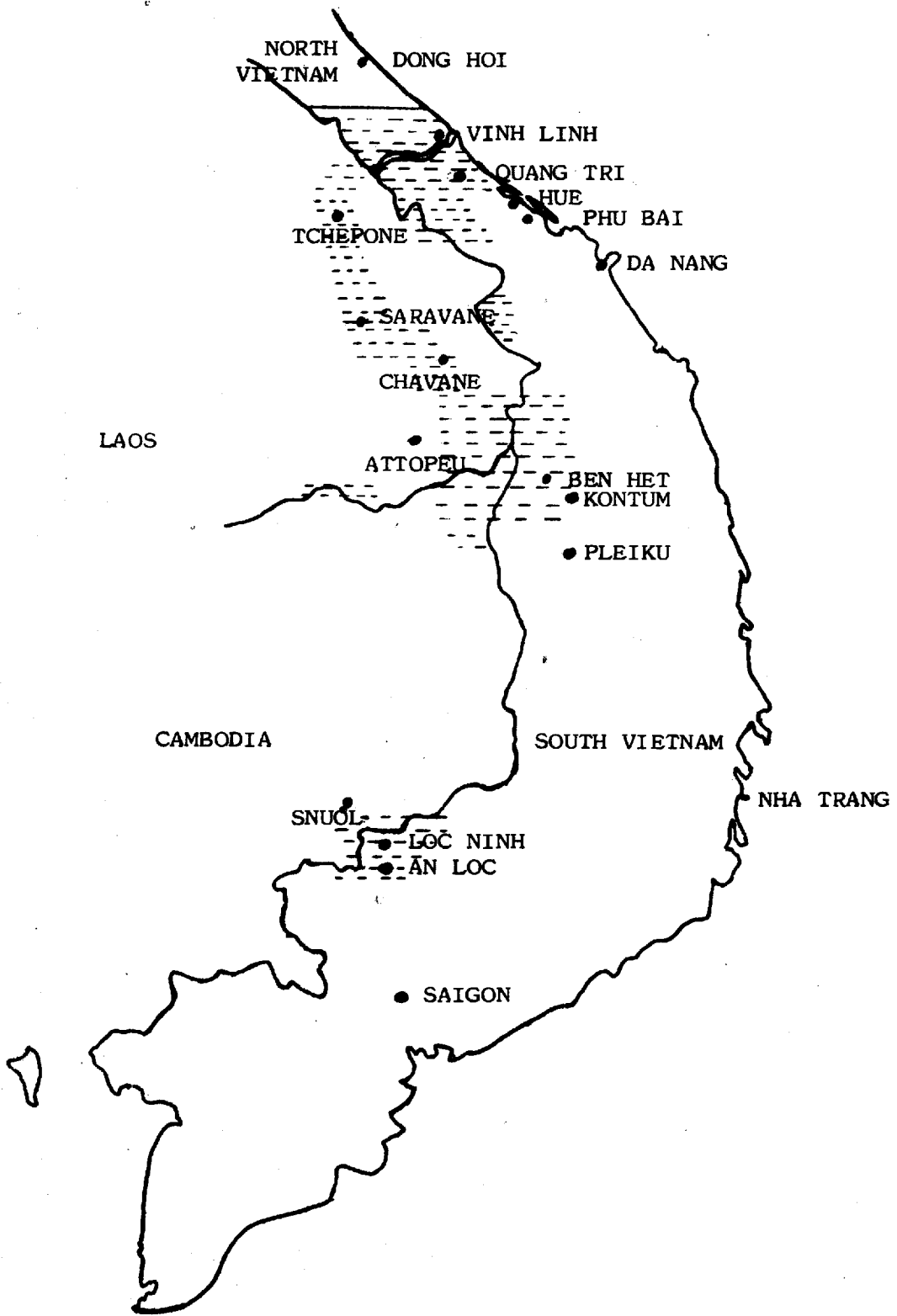
Subsequent assignments in the Office of Southeast Asia Communists have led him progressively from Chief of Southeast Asia Non-Communist Nations Division to his present position as Chief, B6 (Office of Southeast Asia Communists). As Chief of B6, Dr. Jackson has been responsible for guiding the SIGINT activities which support U.S. tactical commanders in South Vietnam, as well as theater and national level decision-makers. In recognition of his achievements in this area, Dr. Jackson was recently awarded the Exceptional Civilian Service Award.


\*\*\*\*

"A good supervisor is one who can step on your toes without messing up your shine."

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



 Tactical areas of operation for NVA armor units

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605THINGS THAT GO CLANK IN THE NIGHT

by Mike Hricik, B61

In late January 1972, the COMBAT APPLE, Laos mission, [redacted] staging from [redacted] began intercepting a high HF radio emission emanating from either North Vietnam or adjacent Laos. Subsequent analysis of this signal indicated to us that it was in the frequency range of the Soviet R-113 radio. throat microphones were being employed, and [redacted] was being used. The correlation of this information suggested that the source of these transmissions was North Vietnamese tanks, a long sought target of the cryptologic community. At first, it was thought that these communications were part of night tank maneuvers in southern North Vietnam. However, as more information became available, it became apparent that they were actually serving large numbers of NVA tanks and armor associated vehicles traversing the southern Laotian Panhandle, enroute to an unknown area of South Vietnam. The following is the methodology used to exploit these communications to the utmost degree and to provide accurate intelligence to the consumer and tactical field commanders in Vietnam.

An in-depth analytic attack on the tank-to-tank communications revealed the probable route of movement through the southern Laotian road system. The first group of NVA armor elements, isolated in SIGINT, apparently traversed Route 96 into the Chavane area, proceeded east along Route 966 to the South Vietnamese border, crossed the border in the vicinity of Dak Pek ARVN Ranger Camp, and possibly moved south along National Route 14 into the area of Dak To/Ben Het ARVN Ranger Camp. The methodology used to ascertain the route of movement for these tanks was rather unorthodox because this was the first observation of actual tank-to-tank communications in Southeast Asia; there were no guidelines available, and a normal traffic analytic approach could not be used. Kilometer markers, mentioned in text, were the beginnings of the jigsaw puzzle. Available information suggested that kilometer markers 69 to 104 were located along one of six roadways in the Laotian Panhandle and adjacent South Vietnam. The roadways were Routes 1032, 548, 128/911, 96/110, 966, and 22/99. The aircraft position at the time of intercept and other anomalies inherent to these communications eliminated Routes 1032, 128/911 and 22/99.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

MEDIUM TANK T-54A



- CHARACTERISTICS -

Weight	40 tons
Length (w/o gun)	21.2 feet
Width	10.75 feet
Height (w/o AA MG)	7.9 feet
Speed	30 mph
Fuel Capacity (w/aux)	141 gal (215 gal)
Cruising Range (w/aux)	216 miles (310 miles)
Main Armament	100mm Tank Gun

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Movement directions mentioned in crewmember conversations yielded another key, since it was reported that when the vehicles reached kilometer marker 102, they were to turn right and head south. Collateral revealed that kilometer markers 102 on both Routes 548 and 96/110 are located on straight segments of road, thereby eliminating these routes as candidates. Collateral also showed the location for kilometer marker 102 on Route 966 at YC 763031, where the road takes a sharp right turn to the south and enters South Vietnam. This information, combined with references to fording streams, crossing bridges, etc., suggested that Route 966 was the most likely avenue of deployment for these tanks.

The initial ARDF fix on an R-113 terminal was obtained on 18 February, positioning it in the extreme southeastern portion of the Laotian Panhandle. Later groups of NVA armor elements appeared to use Route 96 into Chavane, then continue southeastwardly along Route 96/110 into the international tri-border area. ARDF support traced this movement and subsequent groups of NVA armor were located in the Binh Tram (BT) 37, BT 35, and BT 44 areas, Chavane, Saravane, and immediately west of the tri-border area. One group of NVA armor elements was located by SIGINT in the Ton Le Kong River basin near the Cambodian border, approximately 100 kilometers west of the Laotian/South Vietnamese border. The position suggested that this group was not destined for the NVA B3 Front area of responsibility in the central highlands of South Vietnam but, in fact, continued to move southward into Cambodia, transiting the COSVN-controlled areas, possibly with the ultimate objective being the An Loc area of South Vietnam. Collateral reports indicate that NVA T-54 tanks played a vital role in the siege of An Loc that began in early April. There was only one SIGINT location of an NVA tank within the boundaries of South Vietnam, and that was in the area just northwest of the Ben Het ARVN Ranger Camp. This fix was later confirmed by photo-intelligence on the same day.

During the period 3 April to 24 April, no NVA tank-to-tank communications were observed emanating from southern Laos and adjacent Kontum Province, South Vietnam. Two possible explanations for this hiatus are that these tanks and armor associated vehicles had completed their deployment to their destination and were preparing for tactical activity in the area of Kontum City or that these communications were of such low intensity that they could not be intercepted.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

AMPHIBIOUS TANK PT-76 (MODEL 2)



- CHARACTERISTICS -

Weight	15 tons
Length (w/o gun)	22.6 feet
Width	10.4 feet
Height	7.2 feet
Speed (land/water)	27/6.2 mph
Fuel Capacity	145 gal
Cruising Range (land/water)	160/62.5 miles
Main Armament	76mm Tank Gun

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

On 27 April, in north-central Quang Tri Province, R-113 communications revealed combat preparations for an attack on Trung Chi, a village approximately 8 kilometers west of Quang Tri City. Subsequent collateral indicated that, on 28 April, this village was overrun by an NVA infantry attack spearheaded by a number of tanks.

In late June, NVA tank-to-tank communications, possibly in an area east of the A Shau Valley in Thua Thien Province, revealed offensive activity against an unspecified ARVN outpost. These communications disclosed movement of tanks into the combat area, tactical positioning of infantry support, the initial assault, regrouping and maneuvering for the final assault, which apparently was successful.

During late July and early August, SIGINT traced the movement of at least 20 NVA tanks from North Vietnam into South Vietnam. These tanks were initially observed in central Ha Tinh Province on 22 July and, by 1 August, they were located approximately 30 kilometers north of the eastern Demilitarized Zone. At this point, this armor group was instructed to move directly into South Vietnam as quickly as possible. SIGINT followed this group for 11 days as they moved approximately 200 kilometers. As bits of information flowed in and were pieced together, it was almost possible to plot the daily progress of the group.

Collateral and captured documents identified the NVA armor units operating in South Vietnam as the NVA 202nd Armor Regiment tactically committed against Quang Tri and Thua Thien Provinces and the NVA 203rd Armor Regiment supporting NVA offensive activity in the central highlands. Additional collateral indicates that approximately 300 NVA tanks have been destroyed by the Allies in North Vietnam, South Vietnam, Laos, and Cambodia. SIGINT played a vital part in locating these tanks, assessing their strength, and suggesting the final destinations of these armor groups as they were deploying.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

SIGINT AND AUTOMATIC DATA PROCESSING  
by staff writers

The SIGINT industry, as any other business, has an ever-present need for improvement and progress. We want better quality in our information files, and we want information quicker, with more accuracy in detail, and with greater ability to fuse information from various sources. We want to increase the quality and quantity of product from the material we now collect. We also want to collect more, not only of the traditional material, but of new types of signals and radiations as well. In order to handle these increased inputs, we need greater processing capability and capacity. Further, we have to find a way of increasing our output within constraints on manpower and money. Automatic Data Processing (ADP) is the essential resource which significantly expands the capabilities of relatively fixed numbers of personnel within the SIGINT industry. ADP by its very nature promotes systematic treatment of input and output and, therefore, is consistent with the scientific or exhaustive approach to problem solution.

Present day SIGINT would be impossible without computers, for they enable us to get on with the task of analyzing more material, arranged and ordered for the analyst to use. Rarely are we able to reduce numbers of people--instead, a difficult task that could not be done otherwise is done, and consumers' requirements for timely SIGINT can be met that would not be possible by hand processing. We anticipate even more use of "data bases" (our accumulated communications information) in the future that will be ever-expanding in size as well as diversity of content. These will enable preparation of more comprehensive SIGINT reports, both technical and intelligence, than would otherwise be feasible without drastically increased numbers of people.

Without machine assistance, analysts are inundated with a variety of apparently unrelated pieces of information which, due to the large volume, may never be pulled together to exploit the relationships which almost assuredly exist among them. A great deal of available intelligence would never properly be recovered in time to be useful.

To be more specific, here are two important examples of results due to computer capabilities.

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

a. One is to handle large volumes of material. The important fact is that this is not material neatly classified in obvious categories; in many cases it is data which appear completely random in character. Computers alone can deduce non-randomness quickly to help solve a callsign or encipherment system.

b. The other important result is the capability to deal with numerous diverse elements of information, compare them--with each other or as they change form--by a very large number of repetitive trials, and establish relationships previously completely obscure. The establishment and maintenance of traffic analytic continuities is an example of this type of capability.

Two examples of a somewhat different character illustrate the advantage the computer provides in rapid information retrieval. The TEXTA file allows immediate retrieval of basic data for intercept assignment and traffic identification. The new programs dealing with intercept evaluation provide near real-time management of intercept resources in a most effective way.

In cryptology, computers are "expanding our intellect," just as machines earlier gave men capabilities that they could not have with their own muscles. Computers are enabling us to do things that people can't do easily or at all--working with large volumes of material, and comparing many elements of data rapidly enough to give information for further intelligence evaluation in time to be useful in areas of overall importance, national decision-making both diplomatic and military.

\*\*\*\*

*"The reason some people don't recognize opportunity is because usually it comes disguised as hard work."*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

SEADEV--MECHANIZATION FOR T/A DEVELOPMENT

Allen L. Gilbert, B63

The direct support of U.S. tactical units in Southeast Asia created a requirement for the rapid development and identification of unidentified Vietnamese Communist communications. The existence of a combination of guerrilla and main force type units produces a broad variety of signal plan usage, and therefore a high rate of unidentified material. In a tactical situation where many enemy units change signal data to avoid detection prior to movements toward new operational areas, the responsiveness of identification and re-identification can be evaluated in terms of human lives.

In order to develop the needed responsiveness, B6 created the Southeast Asia Development Program (SEADEV), providing mechanized processing for large amounts of unidentified intercept on a daily basis. The intercept is reported daily by field intercept units in the Southeast Asia Technical Summary (SEATS), a formatted reporting vehicle forwarded electrically to NSA.

The incoming SEATS is automatically placed in the machine system at NSA and unidentified records are matched against the data bank for all identified communications. Activities for which both the transmitter and receiver callsigns match those of identified case notations are supplied with that notation and tagged for the appropriate analytic element. The remaining unidentified material is run against the callsign bank containing the recovered books and pages of the Vietnamese Communist callsign system, and placements (book and page, row, column) are added to the records.

Vietnamese Communist signal plans are of great variety and degrees of sophistication ranging from daily changing, basic-generated callsigns, through a multitude of date repeat patterns, to fixed callsigns. Since a large number of these plans involve either daily changing or pattern extracted callsigns from specific books of the callsign system, the unidentified SEATS records are sorted daily by the book placement of the transmitter callsign. Developmental analysts are assigned responsibility for exploitation of specific books and receive daily listings for their areas of responsibility.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

As data repeats within a 90-day depth of SEATS, the records build and the analyst compares it with known users of particular books, with message types, and with Airborne Radio Direction Finding results to determine if it is part of an already identified activity. If the data is identifiable, it is turned over to the appropriate case analyst for development with his other identified communications. Material which cannot be identified, but which meets criteria for case notation, is appropriately notated, and the pertinent data is incorporated into intercept and traffic identification aids which may produce identifications on other uncased SEATS entries subsequently received. The case is then turned over to area development analysts supporting field collection management authorities. Here it is placed on wideband recovery assignment and on developmental positions in the field to expedite the identification through greater intercept coverage. As the coverage builds the case material, many of the developmental activities can be associated with known entities and assigned as part of an entity which is in the regular intelligence reporting cycle.

SEADDEV has not only supported the identification of new communications, but has been invaluable for recovery of communications changes. The resolved data also becomes part of other machine programs supporting the effort against the Vietnamese Communist target.



"And furthermore, I read it in *Dragon Seeds!*"

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

CRYPTO-SCRAMBLE

*Richard Atkinson*

Unscramble each of the five numbered crypto-scrambles, placing one letter in each space, to form five words or names, each of which fits the definition to its right.

1. LEGFRONDS  
--\_O-O\_--

Classical polyalphabetic system using the first 10 rows of a Vigenere square.

2. TRUEPEAR  
--\_O-O\_--

Grille window.

3. SHIPROOM  
-----O

A sequence which has the same pattern as another sequence.

4. POETWORDACT  
\_O\_ \_O\_ \_O\_ \_--

Requires both an enciphering and deciphering device.

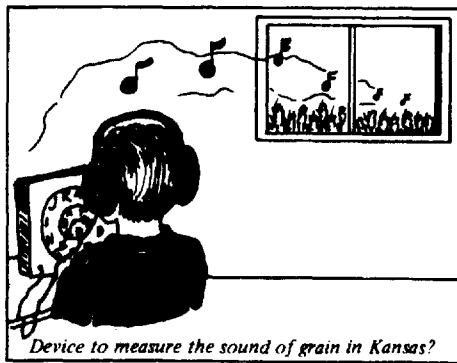
5. DRYOMENS  
--\_O\_ \_O\_ \_--

RYE program which tests for monome-dinome substitution.

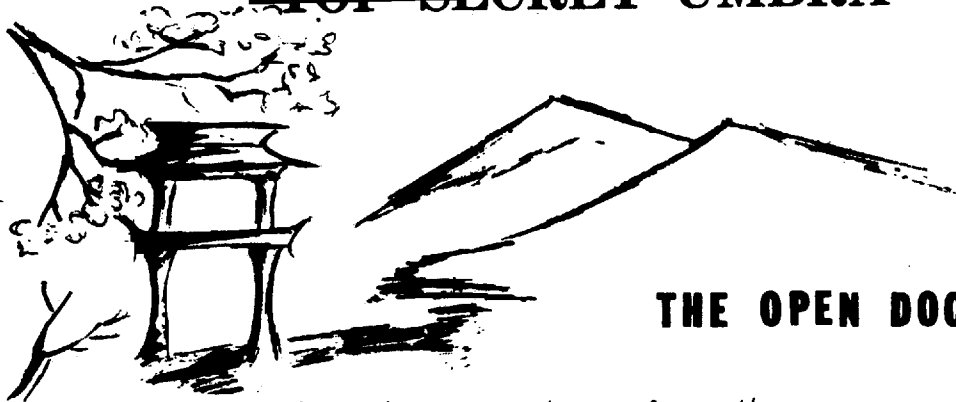
Now arrange the circled letters to form the cryptoanswer suggested by the cartoon at the right.

Print CRYPTOANSWER here

-----



Answers on page 29

~~TOP SECRET UMBRA~~**THE OPEN DOOR**

*We seek to be companions along the way.  
 The lantern which we carry is not ours.  
 The spirit which we share is contagious thought;  
 The knowledge which we gain, an illuminating torch  
 And all who seek may perceive and learn.*

*-The Concept of Dragon Seeds*

PROJECT KAY--OR ANOTHER KIND OF RYE  
 by Louise Swanson, C5

Recognizing that the RYE-AUTOLINE system would not be able to support all potential automatic decryption processing, C Group provided for development of Project KAY as a complementary system. Messages suitable for Project KAY are those in cryptosystems whose decryption would require excessive RYE resources and those whose priorities normally permit the accumulation of messages for several hours before decryption. With the expectation that G Group would be the largest initial user, the development of this processing system was assigned to C53, the division responsible for servicing G Group. Project KAY has been operational for more than two years in various forms on increasing traffic volumes of G Group targets. Both electrically-forwarded traffic and messages on special-source magnetic tapes are being decrypted automatically daily.

Electrically-forwarded traffic being processed includes diplomatic messages in both ILC and national net traffic, the latter being STRUM-formatted in accordance with TECHINS 1022. This traffic is automatically routed from the comm center to the Field Data Processing area in C7. Here it is put through a communications handling system that provides batches of input data to Project KAY several times daily. Electrical data that arrive during afternoon and night hours (between 1100 and 0600) is processed at 0200 and 0600, and decrypts are available by 0730 and 0930. Electrical data that arrive before 1100 daily are usually decrypted and available by 1400. Diplomatic

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

messages from various special sources are received on magnetic tapes at NSA; these messages are normally processed and identified in C6 before distribution of the hard copy is made to OPI analysts. The messages are also retained in machineable form and are available for automatic decryption within a few hours after arrival. Since most of this special source traffic arrives after 1500 daily, it can be processed at night with the electrically-forwarded traffic and the decryptions made available each morning, often before the hard-copy version has been completely distributed through normal channels. A small volume of AG-22 traffic is being handled by the system, but it currently requires some human intervention.

Project KAY processing divides into several steps. Input is a data stream consisting of all messages available from a particular source(s) on many target nationalities. In the first step, the program isolates individual messages in the data stream, determines the nationality of each message, and identifies the message externals. The second step is selection of messages for further processing according to nationality (target designator). Only those messages on targets where at least one cryptosystem can be read automatically are processed further. Messages are identified by cryptosystem in the third step, and the text of those that can be read is completely edited and formatted for input to the last step--the appropriate decryption program. Format flexibility has been incorporated in the editing procedure so that existing decryption programs can be used within the KAY system.

Automatic decryption through Project KAY can be made available for non-G Group targets upon request; requirements should be forwarded to appropriate C5 support divisions.

One such "non-G Group" application has been tested by C55 in support of the [redacted] During July and August 1971, Project KAY successfully identified several [redacted] messages and edited them for subsequent on-line decryption via the Project RAPIDS program TWIST. Project RAPIDS is a set of general crypt diagnostic programs on the IBM 360/85. Combining KAY and RAPIDS processing against the [redacted] messages demonstrated the usefulness of Project KAY to B12, since it made automatic decryption possible with a minimum of custom programming.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

A SOFTWARE APPROACH TO SCRIPT PROCESSING: THE WHY  
by Robert F. Kreinhedér, B12

Most indigenous languages of B12 [redacted] employ what are often termed exotic writing systems. Characters which are bizarre to Western eyes are written in various combinations and juxtapositions to form syllables, of which tone indicators are a part. Unlike the Roman or Cyrillic alphabets, whose letters are written in consecutive order, characters of these languages [redacted] are written in irregular patterns with some characters written above or below others. Since the number of characters involved is also larger, unique Morse equivalents must be used in some languages when communicating. Barred letters are used by collection personnel to represent the unique Morse characters. Some languages have no standardized method for spelling plain text in communications, but employ cipher equivalents instead.

There has long been an interest in developing the capability for machine scripting of B12 [redacted]. In some countries, various entities (e.g., military, guerrilla) now use different equivalents for the same language, making the common script representation very desirable. With the increasing reliance on machine-supported analysis and machine decryption of cipher messages, there has been an increasing need for standard scripted output.



Presently, the JUNGLE BOOK project is being launched to develop CAMINO-type machine dictionary files for B12 languages. This project should be a great help in alleviating the paucity of dictionaries and glossaries and should substantially assist efforts to exploit message texts. It is essential that published versions of these JUNGLE BOOK files employ native scripts. The use of script is also desirable for working aids and training materials so as to eliminate the confusion and difficulty that artificial representation entails.

The languages involved-- [redacted] --have different, if sometimes related, character sets. Print chains for these languages have not been available at NSA and, indeed, their acquisition could be somewhat

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

impractical because of the limited volume involved, the number of different languages, the large size of the character sets, and the irregularity of character placement patterns and printing motion. At this time, a set of practical programs, using available machines, is being developed to accomplish scripting by machine. The linguist's contribution to this process has been to draw and plot the characters using readily understood procedures; provide the programmer with necessary data on alphabetic order and syllable construction; and provide frequency statistics to control internal access priorities.

B12 has been fortunate to have had among its personnel a skilled programmer with interest and enthusiasm to pursue the scripting problem successfully. In the following article he explains his approach to programming toward this goal.

ກ K	ຂ KH	ຄ KHZ	ງ NG	ຈ CH	ສ S	ຊ SZ
ຟ PHZ	ຟ FZ	ມ M	ຍ J	ຣ R	ລ L	ວ V/UA

4060 Lao Output

**ກຳແພງນະຄອນໃຫ້ໂຮງບ  
ທະຫານບຸ້ນຶງວຸດນາມເບ**

Lao Newsprint

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

A SOFTWARE APPROACH TO SCRIPT PROCESSING: THE HOW  
by Ferdinand J. Reinke, Jr., Bl2

The concept of producing non-standard script on a computer can take two approaches: hardware or software. The hardware approach is to modify a printer in some semi-permanent fashion. The software approach uses the computer to automatically control a device to form characters. The purpose of script representation is to achieve several of the following goals: 1) give usable machine output to a linguist; 2) achieve standardization in languages where there is a non-standard Morse equivalent; 3) give the linguist a standard reference for languages with non-standard transliterations; 4) provide a method whereby novice linguists may become immediately productive; and 5) provide non-Roman linguists the same services available to Roman linguists.

The hardware approach has two kinds of problems: first-time setup problems and each-time recurrent problems. The initial problems are designing a font, setting up a metal die, producing the print train, verifying and correcting errors, and establishing a Universal Character Set (UCS). The each-time recurrent problems are removal of the "standard" print train, alignment of the printer timing disk, installation (drop-in) of the print train, loading of the UCS buffer which prints the characters, and verification of the printed copy. Yet, for high-volume needs such as Russian Cyrillic, this approach is perhaps the most efficient. Another hardware approach is the electrostatic ink jet printer. This method uses an electric field to control an ink flow on the paper. The drawbacks are the prohibitive cost, the fact that the state of the art is not advanced enough to support it, and it does not produce subscripts or superscripts.

The software approach assumes 1) the system should be language independent, with the program written in a high level symbolic language to make it compatible across systems; 2) the program's machine and system must be independent; 3) the output microfilm will save space and have several other uses; 4) the program will be usable to a non-programmer; 5) the size of the image should be controlled by the user; and 6) the program should be modifiable as to directional flow, i.e., left to right or reverse and top to bottom or reverse.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

အပထ အောင်စာ

ရန်ကုန်တိုင်းမှ(က)စာရ

ဘာသာဂုဏ်ထူး ၁၂၅ နှင့် ၄

ရန်ကုန် ဌာန ၂၀၁	၁၉၇၁	စာမေးပွဲသို့
ခုနှစ်ပတ်လက်က ကျင်းပခဲ့သော အခြေခံ	ပြေဆိုခဲ့သူ ဦး	
ပညာရေး အထက်တန်း စာမေးပွဲ	(သုံးစသော)	
ရန်ကုန်တိုင်း အောင်စာရင်းကို ပညာ	ထုတ်ပြန်လိုက်	
ရေး ဌာနမှ ယနေ့ ထုတ်ပြန် ခြေပြာ	အရ (က)	
လိုက်၏။ (က) စာရင်းဖြင့် အောင်	ပေါင်း မှာ	
မြင်သူ ၁၁ ခယမ ၉ ခုရှိခဲ့ပြီး	ထောင်စကုတ်	
၅၅ (၈) စာရင်းဖြင့် အောင်မြင်သူ	ဖြင့် အောင်မြင်	

၁	၀၀	၀၀	၀၀
၆	၀	၂	၂
၅	၂	၂	၂
၃	၃	၄	၃

Burmese Newsprint

4060 Burmese Output

แ	บ	อ
ค	ฝ	ล
ข	ต	ก
ฉ	ฉ	ฉ

# เรื่อบจีน

ทางการอเมริกันยอม เราไม่ได้ต้องการ  
 รั้วว่า เรื่อกว่าที่นระ ที่กระทรวง กษา  
 เบ็คของจีนคอมมิวนิสต์ ความเห็นว่า เพื่  
 จำ ๑ ได้เข้าไป ในเขต นั้น เราไม่จำเค  
 เมืองท่าไฮฟองของเวียก ความสำคัญอะไร  
 นามเหนือแก่สปีคาคีที่ อาจหมายถึง การ  
 แล้วแต่ไม่ได้พบขาม ไรเรื่อบ่า ๑ พาร

4060 Thai Output

Thai Newsprint

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The pioneering work done in the Chinese and Japanese languages is slightly different from what is needed. In Chinese and Japanese, one character represents one idea or unit. However, in any alphabetic language, spacing immediately comes to the front. To further add to the complication in Southeast Asian languages, script is not restricted to one line of sequentially progressing letters. So here lies the problem, a low volume user with a non-English alphabet, complicated by tones and other special marks, who needs to see his language in script form.

The full system is designed to run on the IBM/370-165; but since the programs are written in Fortran, the system should be moveable. The user has to design his input equivalents using circles, arcs, and straight lines. This table of equivalents is all that relates the programs to a particular language. Being language independent means any user can design and implement his target language script without any programming.

The script is produced on the Stromberg DATAGRAPHIX 4060, which is a COM (computer output microfilm) device via the Integrated Graphic Subroutines Library on the 370. Microfilm is then available for printing or can be used directly as a viewing medium.

The 4060 is the logical choice for the device to be used for the following reasons: It is 1) capable of doing what is needed; 2) in-house; 3) underused; 4) flexible and adaptable to different uses; and 5) programmable using what is immediately available.

The actual "how-to-do-it" mechanism is as follows: design a character set inside a rectangle on graph paper. Next break the character into a series of circles and straight lines. Then verify the machine's output and modify as necessary. That is the setup before processing material.

It is our goal to provide the facilities to create dictionaries, traffic, working aides, decrypts, reference manuals, and training materials.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

MACHINE-AIDED TRANSLATION

Norman Wild, B03

*In this, the second of three articles on translation and the machine, Mr. Wild sets forth some necessary considerations for the decision to use or not to use the computer as an adjunct to translation.*

AUTOMATIC LOOK-UP

A more modest goal than full machine translation is automatic look-up in which the machine identifies words (or units of look-up) in the text, locates the target-language meaning on a dictionary tape, and prints the meaning. At its best, automatic look-up saves the translator a lot of time in thumbing the dictionary and prevents errors that might be made by a translator who was oversure of his knowledge or unwilling to bother to consult a dictionary.

There may be fringe benefits. The printout of the dictionary tape can serve as a desk aid; the looked-up words can be flagged for subject matter interest and could further provide English equivalents if desired; word frequencies can be tallied; definitions can be evaluated in context; no-matches will show what words are missing from the dictionary; and so on:

Without going the whole way, there is semi-automatic look-up to be considered. In this procedure, the translator enters the word into a computer, perhaps by way of a keyboard, and the definition is printed out or appears on a scope. The advantage of semi-automatic look-up over thumbing a dictionary is that the tape is easier to update and the program can find distorted or incomplete words. The advantage over full-text look-up is that the experienced translator, who should know when he needs help, is not getting a lot of information which he does not need and which costs money to provide.

There are some disadvantages to using automatic look-up in addition to the obvious costs of preparation and operation. The look-up may encourage the translator to rely on the English printout rather than to study the language or at least to go to other dictionaries which would be more informative. It may even

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

encourage attempts by people who do not know the language at all to piece a meaning together from the stream of definitions. That could be disastrous!

When, then, should we use automatic look-up? It is feasible and desirable under certain conditions, and a table of indications and contraindications may be set up. (Note that automatic look-up shares many of the difficulties of machine translation.)

PRO

1. Dictionary in machinable form is already available, or preparing one is desirable for other reasons--usually to print out a desk dictionary when no available one is satisfactory.

2. Input language is already in machinable form or has to be put in this form for other purposes. It may be that the input is available as a by-product of other operations.

3. Spelling of input language is consistent and compatible with the spelling on the dictionary tape.

4. Units of look-up are easy to find in the stream of text. Word-spacers are sent; a code group stands for a well defined word or phrase; etc.

CON

1. Machinable-form dictionary is not available and would not serve any additional purpose.

2. Language would have to be punched or typed for this sole purpose.

3. Spelling is inconsistent and causes ambiguities and difficulty in equating to the form on the dictionary tape. The inconsistency could arise from ignorance, cryptographic constraints or options, lack of hard rules in the target language, lack of standard Romanization or Morse, etc.

4. Text is a stream of syllables or smaller units (down to letters) without word divisions, and words have to be found in the stream by unwieldy tests which are not always reliable.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~PRO

5. Base form is not changed much or at all by inflection.
6. Translators are comparatively untrained and inexperienced and are slowed down considerably by lack of vocabulary.
7. Much vocabulary consists of technical terms with neat English equivalents.
8. There is much need for "extra-linguistic" information such as latitude/longitude of placenames, brief descriptions of personalities, arbitrary standard translations, expansions of abbreviations, etc.
9. Large vocabulary is used because of subject matter (e.g., industrial, scientific).
10. Volume of text is great enough to make the basic expenditure worthwhile.
11. Translations are not required immediately; we can tolerate the delays in preparing material for machine and waiting for printouts.

CON

5. Base form is changed drastically by inflection.
6. Translators are familiar with common vocabulary and have difficulty only with advanced translation problems which an automatic look-up would not help.
7. Translation problem does not lie in the basic meaning of the word but in the best rendering in varying context.
8. Vocabulary should be familiar to a linguist with a good "traditional" knowledge of the input language.
9. Vocabulary is not larger than a translator can be expected to learn.
10. Volumes are small and intermittent; time spent in preparing the system could not be repaid.
11. Translations are required in a hurry; material cannot wait for batching or technical and administrative delays.

In considering automatic look-up, we need to keep in mind that it is a translation aid only. There must be no presumption that the program finds all words or always defines them correctly or that it solves all grammatical or semantic problems. It is never a substitute for language study, hard work, or common sense.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

---Congratulations are in order. Since the last issue, the following B personnel have been singled out for honors.

Exceptional Civilian Service Award  
Dr. Don C. Jackson, Ch B6

Meritorious Civilian Service Award  
Oscar Steele, B63

Joint Service Commendation Medal  
CAPT Harold E. Joslin, Ch B  
TSgt Charles H. LaFosse, B3  
TSgt Garland E. Freeze, B32  
Gy Sgt Raymond S. Cuddy, B61

\*\*\*\*

---A users' guide for the Lewis System of Diagnostics (LSD) written by Danny Boyter, B03, and Al Verbits, P1, is hot off the press. The guide consists of seven computer programs designed to search for known phenomena in hand systems. It includes data manipulation programs which generate Delta streams, width tests, and various counts. There are also programs which search for indicators and fibonacci key generation. Copies may be obtained by contacting the authors on 5210s or 5296s.

\*\*\*\*

---The National Cryptologic School is offering the pilot presentation of a computer-managed course in FORTRAN IV from 0800-1630 hours daily in Room 1B33, FANX II. There is no registration, scheduled classes, or credit given for the course. Students proceed at their own pace, but must finish the course within five weeks. Those completing the course will be permitted to take the final exam for MP-227 (FORTRAN Programming) and should they pass, will be registered and credited for completion of that course. Interested personnel should contact Mr. Gibbs or Mrs. Garlick on extension 8555.

\*\*\*\*

---The personality parade which introduced top B officials to our readers will no longer appear as a feature in *Dragon Seeds* after this issue. It will be replaced by *Buddha Speaks*, a column which will spotlight those people among the NSA work force whose reputation is so exalted it has earned them the title, "Enlightened One."

\*\*\*\*

---Mathematical Support to Traffic Analysis, a P1-sponsored symposium held in the Senior

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Cryptologic Course Center (FANX II) during May accomplished its main objective, to get Traffic Analysts and Mathematicians talking to each other. B participation was extensive. Ken Cohen, B45, spoke about "CHICOM [redacted] Callsigns;" Foster E. Slade, B3, delved into "Desk Analyst's Math;" and Robert S. Benjamin, B03, not only chaired the panel discussion on the final day of the symposium, he also gave an "Overview of Math Support to Traffic Analysis."

\*\*\*\*

----The RJE Users Group previously sponsored by C7 until its demise in mid-August is being revived under C503 auspices. Willard Davenport, 3655s, can provide additional information.

\*\*\*\*

----Several new exhibits are on display in the Center for the Asian Arts at Towson State College.

One display case is devoted to incense. Featured in the exhibit are incense burners and pipes believed to have been first used for burning incense.

A brief history of incense is also included, tracing its usage as it traveled through India, China, and Japan with the Buddhist religion.

Another display contains an exhibit of Eighteenth Century Japanese netsuke--a device used by the Japanese to fasten their purses to their belts. The Towson display contains several examples of the netsuke, carved out of both wood and ivory, and a brief explanation of how it was used.

Aboriginal wood carvings and weavings are on display in the Center lobby.

The Asian Arts Center, on the fifth floor of the Albert S. Cook Library on the Towson State campus, is open to the public from 10 a.m. to noon and 2 p.m. to 5 p.m. Saturday.

\*\*\*\*

----WIN is Women In NSA.

WIN is a fledgling organization inviting B Group women to participate in special interest groups like Consciousness Raising, Upward Mobility, and Self Education.

WIN is reaching out to you. Contact Olive Bennett, Pl, or Dee Zellers, M3, and WIN!

\*\*\*\*

----Don't forget the Learned Organizations! September begins a new membership year for them. They are offering expanded programs, new activities. They are seeking fresh outlooks, broader participation, intriguing innovations. They need your support!

\*\*\*\*

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

----The Traffic Analysis Career Panel has released several of the old exams, with answers, for dissemination to individuals preparing for future T/A POEs. Mel Johnson of B02, extension 5978s, can fill you in on the details.

\*\*\*\*

----Did you know that the Cryptolinguistic Association is making plans for its second annual "Coffee and Conversation" and is seeking donations of pastries, finger foods, and ethnic dishes? Florence Wagner, B12, is the person to contact if you've a keen desire to flaunt your culinary expertise. Extension 7128s or 6497 black.

\*\*\*\*

----Appearing next in the current monthly lecture series of the Crypto-Mathematics Institute held in the NSA auditorium at 0930 hours are:

- Ralph E. Walker, R5 - 5 Oct 72  
Uses of the Fournier Transform in Digital Signal Analysis  
(SECRET/CODEWORD)
- Charles W. Bostick, G4 -  
2 Nov 72  
Probe Vectors (SECRET)

Dr. Lowell K. Frazer, S1 -  
7 Dec 72  
Cryptographic Decay  
(TOP SECRET/CODEWORD)  
All persons with the necessary security clearance are invited to attend.

\*\*\*\*

----On schedule for the CLA 1972-1973 lecture series are:  
A Human Factors View of Translation:  
James Mathias - October  
Machine Bookbreaking: Affinity between Statistics and Linguistics  
George Wood - November  
Information Transfer: Korean to English  
Henry Sullivan - December  
Translation as a Profession  
Lawrence Murphy - January

\*\*\*\*

ANSWERS TO CRYPTO-SCRAMBLE:

1. Gronsfeld
2. Aperture
3. Isomorph
4. Two-part code
5. Syndrome

CRYPTOANSWER: WHEATSTONE

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



ASK

THE

DRAGON

LADY

Dear Dragon Lady:

I am responding to two letters which appeared in the *March Dragon Seeds*, but which I only recently saw, one from Mr. De Gregorio, B12, and the other from Nang Ha.Nyan, who claims to be in B03. Mr. De Gregorio's first:

Both E1, Language Training, and P16, Linguistic Support, can be of some help in tracking down persons who can give training in the less common languages. P16, in particular, is in a position to tap resources of a wide area usually without a great deal of delay. I suggest that you spell out your needs for training and for working aids as precisely as possible and pass them along to me in a memo.

And Nang Ha.Nyan's:

As far as I know, nothing is being done about expanding the number of languages which are being taught overseas in their native environment from its present, modest one (Chinese). Such training is expensive, but as you said it's also very effective, and perhaps a case can be made for it in other languages, too. Again, my suggestion is to make your needs known. If you write a memo, somebody has to answer it.

JOHN S. LAWRENCE  
Chief, P16

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

The Dragon Lady humbly suggests that when trying to locate experts in the minor tongues of mainland Southeast Asia, Pl6 not overlook the talents of the Justin Morse family, one of the most durable missionary families in the China-Burma Hump who after 51 years of administering to tribes in the "Shangri-La" valleys at the "top-of-the-world" are back in the United States renewing ties with the Christian Church following ouster from their adopted homeland by the Revolutionary Government of the Union of Burma. Through educational and medical as well as religious programs, Dr. Morse and family earned the loyalty of Kachin, Naga, and Khamti Shan tribesmen so much so that until 1965, these same hill peoples frustrated the central government's efforts to serve expulsion orders initiated in 1961.

\* \* \*

Dear Dragon Lady:

I welcomed Kay Swift's comments to the Dragon Lady in *Dragon Seeds*, Vol. 1, Nr. 3 dated June 1972, regarding my article Cryptanalysis Through Functional Linguistics appearing in the first issue of this publication.

DONALD P. LENAHAN, B2

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

## CONTRIBUTORS

AL GILBERT, B63, came to NSA in 1966 after retiring from the Army Security Agency as a CW3. While in ASA, he served in Europe, the Far East, Southeast Asia, and at NSA, working at various times as reporter, traffic analyst, Russian linguist, and cryptanalyst. Mr. Gilbert, who is professionalized as a Special Research Analyst, worked the Vietnamese Communist military problem until July 1972, when he joined forces with B1 technicians probing the vagaries of Korean cryptography.

MIKE HRICIK, B6/B2, initially entered the hallowed portals of NSA as a lowly SP/5 in mid-1968 after a rather lengthy sojourn in the Central Highlands of South Vietnam, where he became an ardent Montagnard aspirant. At NSA, Mike delved into the mysteries of traffic analysis, intelligence analysis, and reporting while earning the reputation of being a very competent Vietnamese linguist. His assignment to Saigon in 1970 and 1971 was under Agency auspices to co-sponsor an NSA people-to-people program. He returned in time to be tasked with the duties of the "Senior Dirty Old Man of B6," duties he has not relinquished yet.

ROBERT F. KREINHEDER, B1203, came to NSA in 1957. He was Chief of the Burmese section from 1961 to 1967 and, since then, has been working as a cryptolinguist on Southeast Asia problems. Mr. Kreinheder holds the B.A. degree from Cornell University and NSA certification as a professional linguist. He has served as Chairman of the Burmese PQE Committee and is beginning work as file executive for the Burmese, Karen, and Kachin machine dictionary files.

SGT FERDINAND J. REINKE, JR., of B12 and the 6948 Scty Sq, USAF, has seven years experience in the field of data processing. He is at present on military leave of absence from American Telephone & Telegraph Company, where he was a member of the Programming Staff assigned to the Computer Operations/Systems Group. While with that Group, he worked extensively with IBM/360 operating systems at various levels. Sgt Reinke holds a BEE degree from Manhattan College and is a member of the Institute of Electrical and Electronic Engineers and of the Association of Computing Machinery.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

LOUISE SWANSON of C53 arrived at NSA in February 1965, shortly after being awarded the B.S. in Mathematics by Purdue University. She is a graduate of the P1 Cryptologic Mathematician Program and holds professional certification as a Data Systems Analyst and Mathematician. During her NSA career, Mrs. Swanson has worked as a cryptanalyst on the Vietnamese Communist high-grade military intelligence system in B6, as a programmer on [redacted] and on various projects in C5. In her present assignment in C53, she provides support for G Group cryptanalytic problems. Mrs. Swanson is a member of the Computer Information Science Institute and of the GEBA Board of Directors.

NORMAN WILD, B03, is one of the Agency's foremost multilinguists. He has been with NSA and predecessor agencies since September 1944, working mainly with Far Eastern languages. (It is reliably reported that he reads STC like plain language.) Mr. Wild's academic background includes the B.A. (1939) and the M.A. in Chinese and Japanese (1941) from Columbia University. He is the author of numerous linguistic reference and training aids within NSA, and has long been concerned with the interplay of computers and language.

~~TOP SECRET UMBRA~~



**REMEMBER....**

**IT'S CLASSIFIED!**

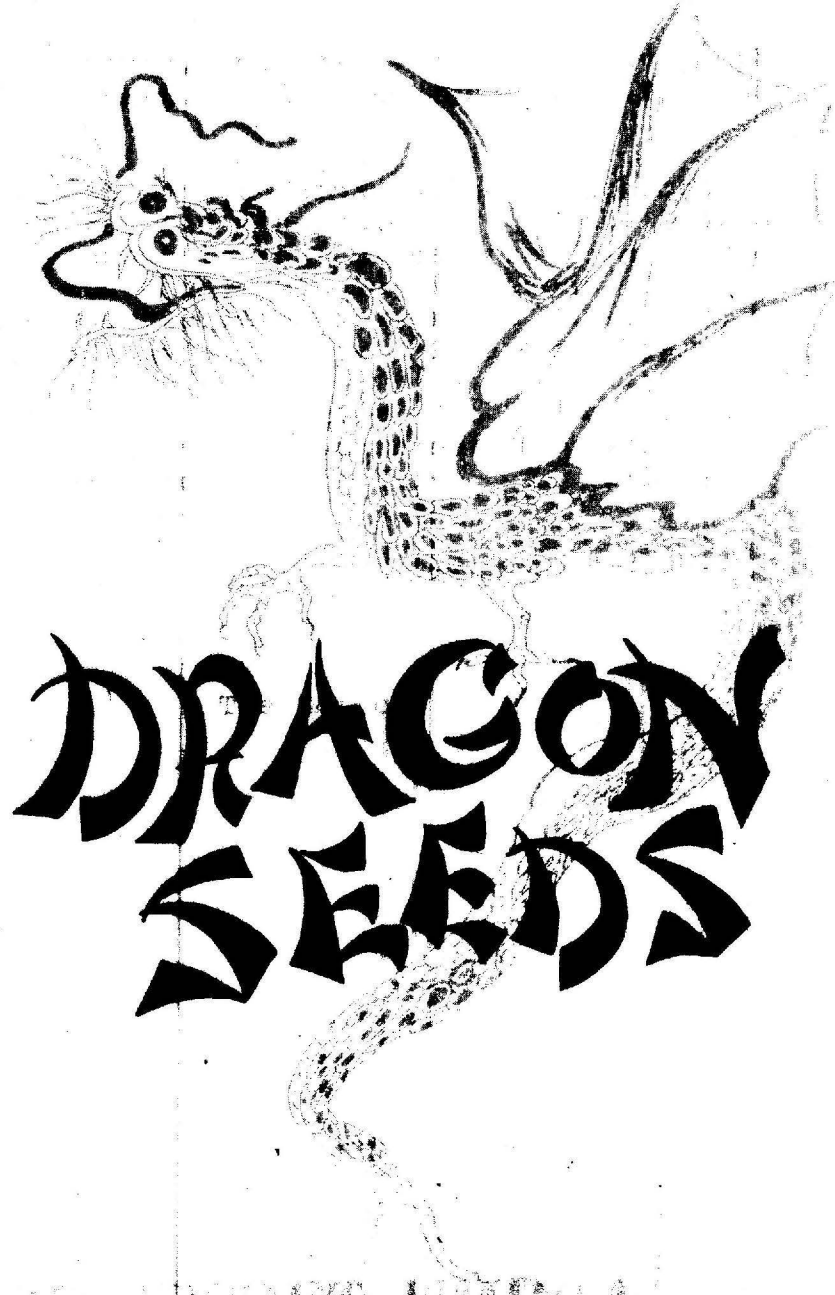
~~TOP SECRET~~

# National Security Agency

Fort George G. Meade, Maryland



DECEMBER 1972



# DRAGON SEEDS

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~TOP SECRET UMBRA~~

This is *Dragon Seeds*.

There is fantasy, irony, and the bite of reality in the name. It speaks of the East. And, like the East, it suggests much, says little.

*Dragon Seeds* is both Mother China and her neighbors. *Dragon Seeds* is monumental and minuscule. It is the past and future. It begs for elaboration but gives none. In it are echoed softly slurred Mandarin, brittle Vietnamese, determined Korean. In it is the spectre looming over the Thai, Lao, and Khmer. It is frightening and friendly. It is uncertain.

Above all, *Dragon Seeds* is promise. It is fertile with ideas unbounded, to be cultivated with creativity and imagination. It is challenge. It is alive. It will be more than it is.

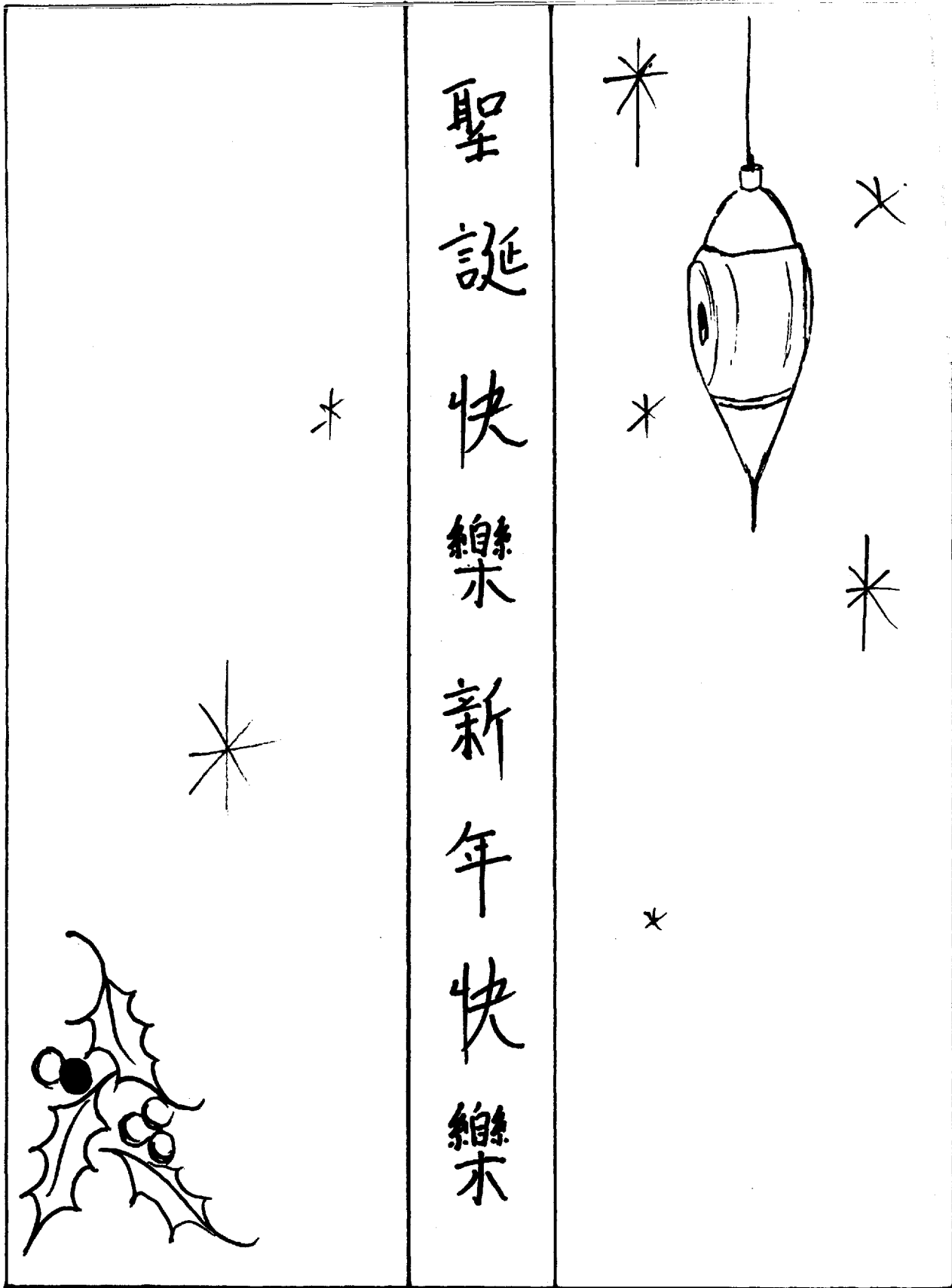
*Dragon Seeds* is yours. May it grow with you.

The Editors

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~


ONE YEAR LATER--DRAGON SEEDS' ANNIVERSARY  
--A Commentary from the Chief, B

It does not seem that long, but Dragon Seeds is now one year old. During its initial year, it has shown development and an enviable standard of excellence. The publication has in many respects exceeded my highest expectations. I continue to be impressed with the varied talents of the personnel in B Group, and each succeeding publication magnifies this impression. The wide variety of interests and technical acumen displayed by the contributors makes me proud of our B Group professionals. I sincerely desire this interchange of experience and ideas to continue.

I feel Dragon Seeds is proving a most effective medium to encourage and stimulate professionalism in B Group. Some of its articles--I recall Things That Go Clank in the Night in the last issue--indicate how important and exciting our results can be. This is a most useful stimulant to the many whose daily results do not have the excitement of vital immediacy--regardless of the longer term importance of their work. There is much appropriate emphasis on mechanization of our problem--an area full of development potential and problems in making complex, computerized systems work. As I look over the contents of our four issues--we have ranged across all our major disciplines and included some interesting reflections on management problems. It is a delight that some of our contributors have provided welcome chuckles--humor needed to lighten our serious endeavors.

However, our Group covers such a wide range of interesting activities that our talented personnel have an inexhaustible range of subject matter for future articles. If you are excited about what you are doing, if you feel you are doing something important, if you see problems needing attention--write about it; share your enthusiasm or concern with me and the rest of B Group. And let's see our Ms's and military personnel participate to a larger degree.

Happy Birthday, Dragon Seeds, and full steam ahead!

  
HAROLD E. JOSLIN  
CAPTAIN, U.S. Navy  
Chief, B

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

## Memorandum

TO : Captain Joslin, Chief B

DATE: 30 August 1971

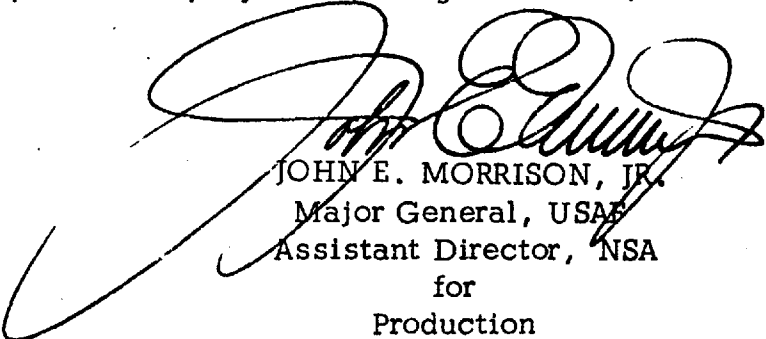
FROM : ADP

SUBJECT: Letter of Appreciation from Major General Potts, J2 MACV

Prior to his departure, Admiral Gayler asked that the attached letter be circulated to appropriate contributors here at NSA, particularly B6.

I happen to think this letter is one of the finest accolades we have ever received from a senior intelligence officer who has been in a outstandingly unique position to earnestly evaluate the contributions of SIGINT to the allied cause in Vietnam. I know of no other organization within Prod more deserving of receiving and retaining the original copy of this letter than B6. I am mindful of the fact that others have contributed, among these P1, P2, C, TCOM, and many other elements of your fine B Group organization. I will see to it that those outside of B Group who are deserving receive copies.

Please make appropriate distribution of copies within B Group at large. You know best who should receive them. Please add to the generous comments of General Potts the deep gratitude of Admiral Gayler and, of course, my own. Congratulations!



JOHN E. MORRISON, JR.  
Major General, USAF  
Assistant Director, NSA  
for  
Production

Attachment:  
a/s

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

HEADQUARTERS  
UNITED STATES MILITARY ASSISTANCE COMMAND, VIETNAM  
APO SAN FRANCISCO 96222  
Office of the Assistant Chief of Staff, Intelligence

4 August 1972

Admiral Noel Gaylor, USN  
Director  
National Security Agency  
Fort George G. Meade, Maryland 20755

Dear Admiral Gaylor,

During the month of August 1972, I will complete three and one-half years as Assistant Chief of Staff, J2, Intelligence for the Military Assistance Command, Vietnam. Therefore, I wish to take this opportunity to extend my sincere appreciation for your personal interest, valuable assistance and timely support in the successful accomplishment of our intelligence mission for COMUSMACV. Throughout this long and critical period the expertise, analytical skill, dedication and devotion to duty of The National Security Agency has unfailingly rendered invaluable aid to me, COMUSMACV and his subordinate commanders. We are most grateful for your many significant contributions to the Free World mission in the Republic of Vietnam.

Sincerely,

*William E. Potts*  
WILLIAM E. POTTS  
Major General, USA  
Assistant Chief of Staff, J2

~~TOP SECRET UMBRA~~

## DRAGON SEEDS

## Publisher

DONALD E. MC COWN, CHIEF B03

## Managing Editor

Minnie M. Kenny

## Feature Editor

Richard V. Curtin

## Rewrite Editor

Victor Tanner

## Executive Editor

Robert S. Benjamin

## Biographical Editor

Jane Dunn

## Education Editor

Marian L. Reed

## Special Interest Editor

Ray F. Lynch

## Composition

Helen Ferrone  
Lorna Selby

## PRESS CORPS

B11 Carolyn Y. Brown

B12 Philip J. Gallagher

B2 Dee Ensey

B31 Jack Spencer

B32 Jean Gilligan

B33 Louis Ambrosia

B34 Thomas L. Wood

B41 James W. Schmidt

B42 Peggy Barnhill

B43 Mary Ann Laslo

B44 Jack L. Thomas

B45 John E. Uzarek

B5 Nancy Fournier

B62 

B63 George S. Patterson

B63 William Eley



Vol. 1  
Nr. V

DECEMBER 1972

**TABLE OF CONTENTS**

Budda Speaks		1
Callimahos.....	Jean Gilligan	3
Uncertain Origins.....	Tom Glenn	5
The CINCPAC Intelligence Coordination Group	Walter D Abbott	16
AG-22: Where Do We Go Now .....	Phil Remsberg	22
The Development of a COMINT Translation Course for Vietnamese Linguists.....	Jack Sharretts	24
The Open Door: Don't Say MUSSO - Say USSID	Louis C. Grant	28
Machine Aided Translation: Part 3 .....	Norman Wild	31
The Wade-Giles System .....	E. Leigh Sawyer	35
T/A - Math Symposium Reviewed .....	David J. Tiren	36
Seedlings		40
Ask the Dragon Lady		42
Contributors		48

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~B  
A  
D  
D  
A  
A

(Editor's note: We asked the Guru of the Dundee Society to grant us a few words of wisdom from his enlightened state of mahasambodhi. What follows is a brief article which appeared in the Hall Herald (Arlington Hall Station) for 9 May 1947. It is reprinted here because of its impact on present-day technology.)

THE MX-14: A VARIABLE INTEGRATOR

A succinct explanation by Lambros D. Callimahos

An engineering Schrecklichkeit of the first order, the MX-14 was unveiled on 23 April before a distinguished gathering at the Arlington Officers' Club. The highlights of the principles of this machine, which was developed under the greatest of secrecy and unnatural tension, may be briefly elucidated as follows:

The five variables (two components of which are continuously variable) generate a point through four dimensions by the simple expediency of binary translation of the development of the linear functions of an ellipsoidal plane, modulo zero. The convocations of the contortion series under the influence of the aberrations of a mellifluous hysteresis induced by partially damped shock waves, result in a progression which may be best explained as a modified Fourier agglutination with mutually exclusive coefficients derived from three variables not specifically represented by Poisson's Law of Small Numbers.

The deviation of the catalytic sums of least squares hardly makes an impression on the generatrices produced by the interaction of factorial deltas in cascade, but on the other hand, the asymmetrical sohamillac touched off by the misalignment of the cycloidal contusions out of phase play havoc with the formation of Lissajou's figures. Furthermore, the recurrence of asymptotes tends to polarize the stronger principles of Bernoulli's theorem; but this can be almost entirely offset by the carefully controlled integration of palpebral saltations.

M  
X  
-  
1  
4~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

There is a difference of opinion whether it is the Gleichschaltung or the Weltschmerzenumkreisung that retards the bar-sinister effluvium, but this point cannot be settled conclusively until all the phenomena of the expansion of differential planimetric clavicles (cf. Homo, Ecce--La Vida Breve, Bologna 1947) have been collated and studied.

Enough has been said here to give the reader a clear idea of the general theory and purpose behind the MX-14. Further discussion will be continued in a classified paper available to personnel who must refer to it in the performance of their official duties. The paper will also include an example of the Pyrrhic occlusions generated by the reflexed undulatory motion of the experimental model of the MX-14.



*The Guru astride his ah...burro in Greece, 1972.*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

CALLIMAHOS...

by Jean F. Gilligan, B32

To encapsulate 60 or more years of a varied and full life and, at the same time, to do a modicum of justice to the subject of an interview is a completely impossible task unless the interviewer finds a kind of universal that will give a single meaning to many aspects.

Lambros Demetrios Callimahos is assuredly a man of many, many parts that can conveniently and honestly be universalized by a reference to Sixteenth Century Sir Thomas More, of whom Robert Whittington, a contemporary, wrote: "A man of...wit and singular learning...a man of marvelous mirth and pastimes..a man for all seasons."

Mr. Callimahos has contributed articles on cryptology to *World Book Encyclopedia*, *Collier's Encyclopedia*, and he has prepared an 11,100-word article for the forthcoming edition of the prestigious *Encyclopaedia Britannica*.

As a scientist, he has written on such subjects as "Cybernetics and Problems of Diagnostics: The Parallels between Medicine and Cryptanalysis" and "Communication with Extraterrestrial Intelligence."

An accomplished linguist, Mr. Callimahos retains and further increases his fluency in seven foreign languages by taking his notes in a different language every day of the week.

Mr. Callimahos does not regard his knowledge as a purely personal possession; in addition to sharing it with others through his numerous publications, he teaches the most advanced course in cryptanalysis given in the Agency. Even in his teaching, Mr. Callimahos exhibits the dynamics of a multitalented individual. His own teaching is not a static, routine activity; it is an ever-alive and changing endeavor, as is evidenced by his ability to teach effectively in four months what once required four years.

According to a *Paris Soir* reviewer, "Callimahos has proved himself to be one of the greatest flutists in the world." *The New York Times* stated, "Mr. Callimahos commands the resources of

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

his instrument to the services of his artistic will." If Mr. Callimahos shares his artistry with his audiences, he does still further sharing by devoting his time and superb talents to the teaching of advanced students of the flute.

Mr. Callimahos does not limit himself to the admittedly esoteric fields of cryptanalysis and the flute; he is a husband and the father of two children, a board member of the Prince Georges series of the Baltimore Symphony Orchestra and of the Prince Georges Symphony Orchestra, and is actively engaged in work for retarded children.

It is not surprising that Mr. Callimahos is no gourmet of pedestrian tastes. He is a member of the Anteaters Association, which banquets five times annually on delicacies such as fillets of hippopotamus, elephant, and whale.

In his work at the Agency, Mr. Callimahos is a staunch supporter of professionalization, stressing the importance of a thorough theoretical training program and follow-up for technical careers in the Agency.

In the age of narrow specialties (and even narrower specialists), it is uniquely refreshing to meet and chat with Mr. Callimahos, who makes the widest possible range of creative human experiences his own overspecialty.

\*\*\*\*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~UNCERTAIN ORIGINS

by Tom Glenn, B6

In October 1967 I was the only American civilian within miles of the military complex at Pleiku, Vietnam. I had just arrived on TDY to work with analysts of the 330th Radio Research Company (USM-604). The unit had been there more than a year. It was ostensibly a mobile outfit and was expected to be able to move on command. It had sat in vans, tents, and temporary buildings through the winter blasts of red dust and the summer onslaughts of red mud waiting for a command that never came. It clung without roots to its allotted slope on Engineer Hill, all sand bags, watch towers, outhouses and barbed wire, listening intently to the Vietnamese Communist transmitters all around it. Only a civilian, I thought to myself, could really appreciate the profound desolation of a military SIGINT unit mired in Vietnam's western highlands.

But the analysts I met were anything but desolate. Working in a pair of tottering quonset huts at tables they had made themselves and harassed by wind, dust, and erratic electricity, they saw themselves in league against the forces of evil--variously embodied in the VC, the weather, and NSA. They were sustained by an irreverent humor and a passionate devotion to their work. Above all, they shared a foreboding of uncertain origins that a major enemy action was in the offing. They felt it in their blood. "It's like when I get a new dinomic substitution system in," a crippe told me. "I can tell what it is sort of by the way it smells."

The analysts and intercept operators to a man worked as if their lives depended on it. Most stayed at it twelve to fourteen hours a day, seven days a week, working against colossal odds. The target defied exploitation. Less than one percent of the traffic was readable, the signal plans consisted mostly of daily changing calls, freqs, and skeds, and the transmitters the Communists used were low-powered and erratic. The traffic volumes were staggering, requirements overwhelming, and customer need unquestionably urgent. Working and living conditions were suited to an infantry unit, not a SIGINT one. Perhaps most debilitating of all were the ungrateful, hungry tactical customers.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

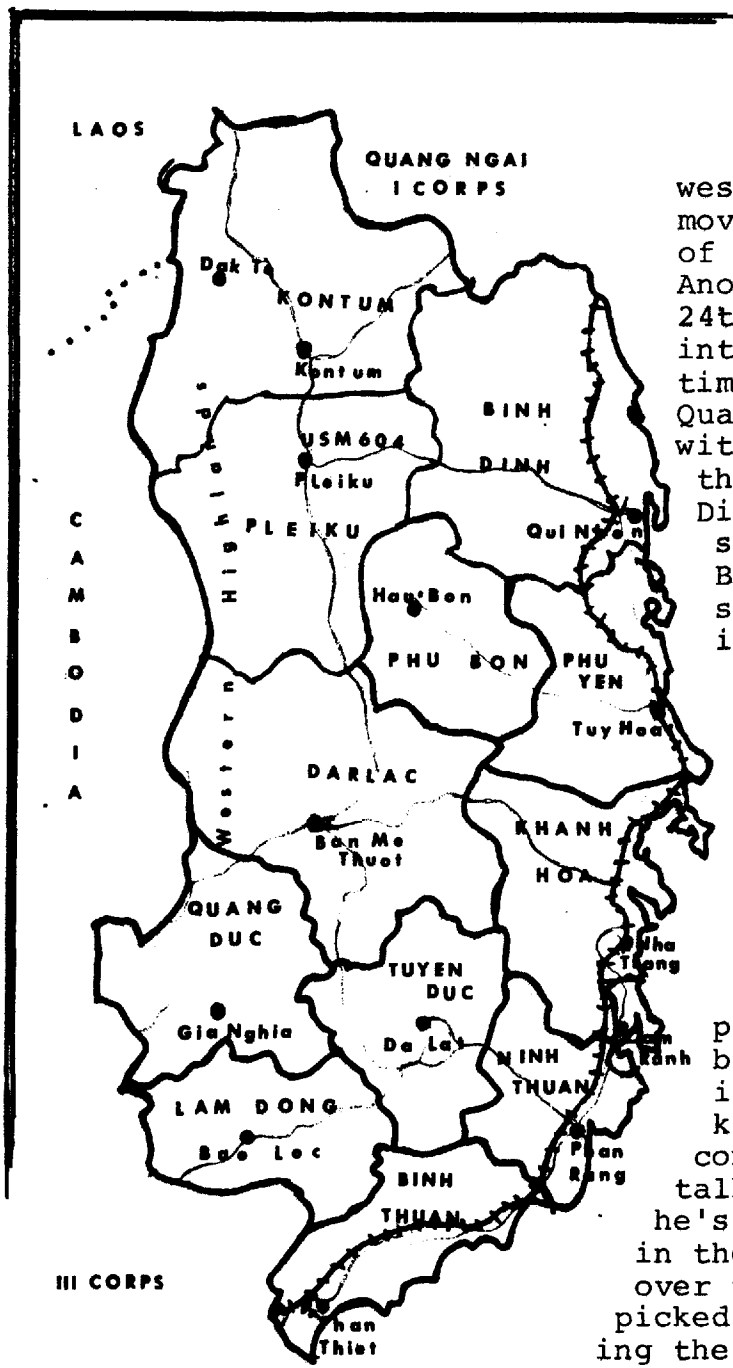
Every Saturday three or four men would go by jeep down the road to Camp Enari to brief the U.S. 4th Infantry Division. The message they brought back was always the same: "They want more SIGINT, they want it faster, they want it in more detail."

That the analysts produced a steady flow of usable intelligence bore witness to their ingenuity and unflagging determination to outflank the elements ranged against them. But I could not help wondering if the presentiment of a coming attack that ran through the company like an underground river was not in part some kind of an irrational outlet for the pressures they lived with day after day. I wanted to know what factual basis there was for their suspicions. Having decided to dig into the SIGINT facts, I started with the traffic analysts.

Bruce Andreason was the senior traffic analyst responsible for the NVA (North Vietnamese Army) B3 Front, the Communist command for the western highlands. He was big, blond, and blunt. "The whole ball of wax is coming apart at the seams," he told me in his characteristic lingo. "Look here. The front headquarters has sent out a new detached element. This new guy talks to Hanoi--that shows you what kind of brass he is--and since 7 October he's been passing and receiving more messages than anybody else on the net. He's been getting messages from the highest echelon headquarters in South Vietnam. Now this guy is some important cookie." Much of this activity, he went on to explain, took place at night when the Vietnamese Communist transmitters are normally shut down. Most unsettling of all, the detached element had moved 77 kilometers north in six days and was now operating northwest of us near the tri-border area--the juncture of the Laotian, Cambodian, and Vietnamese borders--in Vietnam's Kontum Province.

What were the communications of the known tactical units like? Where were they? He shrugged and handed me his intercept logs and airborne radio direction-finding (ARDF) results for late September on. I saw that the communications of the NVA 1st Division, the largest combat force of the front, had been in disarray since 29 September--the day after the new detached element of the front had started communicating with the front headquarters. Communications with the subordinate regiments of the division--the 32nd, 66th, and 174th--were virtually inactive, ruling out any possibility of locating them. But the division headquarters had been located earlier that day (15 October)--in

~~TOP SECRET UMBRA~~



NVA B3 FRONT AREA:  
Kontum, Pleiku, and Darlac

western Kontum Province. Its move there had paralleled that of the front's detached element. Another B3 Front unit, the NVA 24th Regiment, had also moved into the area at about the same time. It had come south from Quang Ngai as if to rendezvous with the detached element and the headquarters of the NVA 1st Division. I began to understand that the forces of the B3 Front were going through some sort of a change, and it smelled tactical.

I turned to the linguists for more information. John Thomas, lanky, bass-voiced, and acid-humored warrant officer in charge of the language shop, tapped the map. "Down here, south of us, is where it's happening." He was pointing at Darlac Province, a full two provinces away from the tri-border. "The 33rd Regiment is getting ginned up. All kind of tactical talk in his comms. Of course he always talks bigger than he hits, but he's a good thermometer of what's in the wind. And up here, just over the hill from us, we've picked up a guy who's reconnoitering the Pleiku area. He doesn't say much we can understand or read, but the idea is clear enough. They're up to something. Not just up in Kontum, but down here, near Pleiku, and then on further south in Darlac."

~~TOP SECRET UMBRA~~

Davy Dawson, the senior enlisted reporter, agreed. "It's not something I can explain to you in any real clear way, but just the way they're acting--all these new low-grade systems since September, the comms structure changes in the B3 Front, the stuff down in Darlac--it just sort of doesn't sound like a long winter's nap, does it?" It didn't.

By now it was the 18th of October. Sam Berry, a new second lieutenant, had been put in charge of the reporting shop at my request. Sam had been a civilian at NSA working the Vietnamese Communist problem, and we needed his know-how. Sam, Davy, and I went to Pop Warner, the senior warrant officer in charge of the analysts, and ran through the facts we'd assembled. Pop, who had more SIGINT experience than all of us combined and enough meanness to work us all under the table, wasn't impressed.

"I suppose you think you're telling me something I don't already know? I respectfully suggest, sir," he said to Sam with a trace of twinkle, "that you report all this." Sam grinned.

"Take a look at this." Sam handed him a draft spot report summarizing what we had so far.

The main weakness of our position, as Pop was quick to point out, was that we were lacking several features that would clinch the evidence that an offensive was coming. If we were right, we could expect that the NVA 1st Division would soon start collecting detailed reconnaissance information on the prospective target (or targets). Meticulous fact-gathering was a normal part of the Communist battle preparation pattern. But the Military Intelligence Section of the 1st Division had been off the air since August. Besides, none of the regiments of the 1st Division had resumed communications with the division headquarters. It was a good bet that they were on the move--their silence indicated that--but where they were going was anybody's guess. We released the report without comment on the implications. And we waited.

One moonless night when we were feeling spooked, we got in a fix on a new unit about 20 kilometers from where we were sitting. We couldn't identify the man, but he was clearly Communist military and the characteristics of his communications made us edgy. We wondered, for example, if he was alone or if other units were with him. One of the B3 Front analysts wrote up a quick spot report on the fix and gave it to me for editing. To save time, I decided to type it for him.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Then I heard the siren. We were under attack. Analysts bolted for their combat gear and took off for their positions on the perimeter. I hadn't the vaguest idea of what to do. I slipped on a flack jacket and helmet and went on typing. The GI assigned to guard the quonset watched me in disbelief.

The lights went out. I heard something that sounded like a child screaming, distant and indistinct. Then came the concussion of the first mortar round impacting. It brought to mind my earthquake days in San Francisco; a little dust fell on my face and the quonset creaked. All there was to do was sit there in the dark and listen to the incoming rounds, my stomach turning inside out, and wait. Twenty minutes later the lights came back on. I heard the all-clear signal. The only casualty, as I was to learn later, was an outhouse. I resumed typing.

I could not have devised a better way to impress the military. I never quite got up the nerve to admit that I had stayed put through the attack from sheer witlessness. And the way I flinched at the slightest sounds later never seemed to undo my credibility. The faint distrust I'd encountered from officers and enlisted men alike disappeared from that day forward. I was welcomed into both the officers and enlisted clubs, I was called into operations at all hours of the day and night just like the military, and everybody stopped calling me "sir." My fatigues showed up with 13's sewn on the collars (I was a GG-13) and my cap was decorated with the unit symbol (much to the confusion of those personnel who didn't know me and were never sure who, if anybody, should salute).

Meanwhile, the Vietnamese Communists were not sitting idly by. Gunships and artillery apparently convinced the attackers that Pleiku was not a lucrative target, but action elsewhere continued.

On 20 October, the cryppies and linguists received a message picked up during search. They diagnosed the system as a dinomic substitution, but it was so short a piece of text they couldn't break it. Several more messages came in during the next two days, and we broke the system. Somebody in the Dak To area of western Kontum Province, it seemed, was in the middle of urgent operations and was afraid that Allied forces might detect it. Finally,

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

through a wideband replay, we got signatures on a message of 23 October. The names were those of the Military Intelligence Section of the NVA 1st Division. The combat reconnaissance we had been waiting for had started. The NVA 1st Division was clearly preparing for an attack--somewhere in the Dak To area of western Kontum Province.

From that point on, things happened fast. Reporters were hard put to pump out the information as they received it. We pinned down the calls, freqs, and skeds of the military intelligence link and identified a fix taken on 21 October as the location of the Military Intelligence Section. It was operating near Dak To and, like the division headquarters and the detached element of the front, it had moved some 70 kilometers north during its silence. On the 25th, the 32nd Regiment was located in the same area. It had moved more than 100 kilometers north since the 16th. On the 27th, the 66th Regiment was located nearby. On the 30th, the 174th Regiment appeared in the same area. Communications silences on the NVA 1st Division net ended as each unit reached its new position in western Kontum Province.

At the same time, cripplies and translators were breaking out and publishing a growing volume of messages exchanged by the military intelligence units of the NVA 1st Division in the Dak To area. On 23 October the Military Intelligence Section passed reconnaissance instructions to subordinates. On 24 October an element expressed alarm at the presence of "commandos" and fear of discovery. A new mission was discussed on the 25th. On the 26th the section told a subordinate about the shifting of Communist forces in the area. The same message instructed the subordinate on communications changes and foretold of a simplified signal plan to be used between 30 October and 4 November. The NVA characteristically introduced simplified SOIs just before combat was expected to begin.

Finally, on 29 October, the section cautioned a subordinate about the need to maintain secrecy to avoid trouble "before it is time to strike." Sam, Davy, Pop, Bruce, the linguists, and I put together a report. It was a summation of everything we had been reporting since the 18th. "The accumulated evidence... strongly suggests that a major tactical thrust is in the offing," we said. We suggested the period between 30 October and 4 November as the probable launch time. The target was to be in the Dak To area.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The next day, the final piece of evidence came to us: the forward element of the 1st Division activated communications with combat units. The pattern was unmistakable: command elements move in, reconnaissance begins, combat forces take their positions, a simplified signal plan is introduced for ease of communication during combat, and a forward element--a tactical command post--takes control of fighting units. The stage was set.

At this point we hit an unexpected obstacle: credibility. Although SIGINT had been used with singular effectiveness to detect Vietnamese Communist attack preparations since 1965, customers remained dubious. On the one hand, there was little or no supporting evidence from collateral sources that the Communists had moved into the Dak To area or that they were planning an offensive of virtually unprecedented scale. On the other hand, the exotic quality of SIGINT analysis and processing, which the customers were in no position to question, made them hesitant. Besides, SIGINT was a new dimension to many of the tactical customers, and the stunning accuracy of the SIGINT community's prediction of the TET offensive was still three months in the future. Customers asked, with understandable reasonableness, what magic allowed a bunch of shaky GIs, distinguished more for their spit than their polish and abetted by an unknown civilian, to use a tangle of antennas and funny talk to divine the combat plans of the enemy?

Nevertheless, U.S. military commanders began to redeploy their forces in the face of the threat. On 1 November, a B-57 strike launched against ARDF locations of major units in the Dak To area brought large secondary explosions. The U.S. 1st Brigade, 4th Infantry Division, established its headquarters at the Dak To Special Forces Camp, and two small close-support SIGINT collection units scheduled moves to the area. On 3 November, the U.S. 3rd Battalion, 12th Infantry air-assaulted into a landing zone on Hill 978, six kilometers south of Dak To, and encountered a large NVA force. The same day, the 3rd Battalion, 8th Infantry, landed on nearby Hill 882 and drew heavy enemy fire. The battle for Dak To had begun.

Before it was over in late November, the battle proved to be one of the biggest in the war. Nine American battalions from the 4th Infantry Brigade and the 173rd Airborne Brigade were committed. Air sorties exceeded 2000, over 1600 NVA were killed in ground combat, and another 500 (estimated) by air

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

strikes. U.S. dead reached 283, South Vietnamese 61. The figures cannot convey the reality of what was going on at Dak To. It began to come home to us when couriers delivering the daily traffic from close support units described orderly stacks of American bodies on the Dak To airstrip. The SIGINT support units were hit; the traffic we worked was sometimes bloodstained.

While the biggest battle was at Dak To, it was not the only one. The Communists also mounted attacks at other points throughout the highlands at around the same time. In addition to the harassment of Pleiku we had experienced earlier, there were probes of varying size throughout Kontum, Pleiku, and Darlac.

A rallier who turned himself in on 2 November eventually confirmed the SIGINT indications of NVA plans and answered some of the questions that had puzzled us. According to him, the NVA 32nd and 66th Regiments were to attack the Dak To area from the southwest while the 24th Regiment acted as a blocking force to the northeast. The 174th was to act as a reinforcing element if required (it was). The original attack date, the rallier said, was to have been 28 October, but coordination problems earlier had made that impossible. From what the rallier said and from other collateral evidence which accumulated later, it appears that the intrusion of U.S. forces south of Dak To took the NVA by surprise and forced them into battle before they were really ready. Documents captured toward the middle of the month during the heaviest fighting indicated that the objective of the offensive throughout the highlands was the annihilation of two U.S. brigades--presumably the 4th Infantry and the 173rd Airborne. The enemy may have planned to use the technique he had employed at Ia Drang some two years before--chewing up battalions one by one as they were committed as reinforcements. The tip-off through SIGINT precluded that tactic. Whether the 1st Division ever recovered completely from the blow is questionable.

A number of things resulted from the accurate prediction by USM-604 of the Dak To campaign. The unit was congratulated by its superiors; the 4th Infantry Brigade was pleased; the analysts were happy; NSA seemed somehow less like a malign uncle; and it was rumored--although I have never been able to confirm it--that the unit was submitted for Presidential Citation. Technically, the SIGINT community gained insight into attack preparations, communications, insight which confirmed several key items on the SIGINT

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

indicators list, which in turn contributed to NSA's success in predicting the TET offensive the following January. Perhaps most important, local customers gained new respect for SIGINT and were somewhat better prepared to accept predictions of country-wide offensives during the next two years.

Despite--or perhaps because of--the grimness of what was happening at Dak To, the strain of the increased volume of intercept, and the rising importance, speed, and number of reports and translations, the men of the 330th continued to refine their sensitivity to the ridiculous. Pop Warner was named chief of the WOPA (Warrant Officers Protective Association) to defend "the real hard-core" against up-and-coming junior commissioned officers. Not to be outdone, Sam Berry formed SLAP (Second Lieutenants Association for Protection), and I was forced to establish an organization all for myself, CLAP (Civilian League for Aid and Protection). There were endless dinner table arguments over whether every second lieutenant needed a civilian and a senior warrant officer to keep him out of trouble or whether it was the other way around. We used the visit of high-ranking personnel as an excuse for a banana dacquiri party and I was treated to a slamming ride along the perimeter in an armored personnel carrier (it ended when Pop drove it over an "unexpected" rise at top speed and I flew completely out of the carrier). My biggest problem was containing exuberant reporters, including Sam, who went so far as to develop the "word of the day"--a term taken from the dictionary that they would try to sneak into their reports when I wasn't looking (I still remember "overweening incipient ambivalence"). My efforts to communicate with the analysts were sometimes confounded by their lapse into a lunatic language which bore only passing resemblance to English: "I can't even hear you," "Don't beg on me," "Just rap, just put it in," and "Civilian nugs are the worst kind." All this was punctuated by the intrusion of barely credible personalities: a sergeant who fancied himself Gunner Asch and took to bloodcurdling yells at odd hours during the mid-shift; a superb linguist who looked like Akhenaten and so worried about every outgoing translation that we named him "Mama;" a mortician-turned-traffic analyst named Digger whose brilliant reports on the setbacks of the NVA achieved the poignancy of a good TV serial; and a collection of domesticated animals that included a monumental boa constrictor named Clarence and several alcoholic dogs.

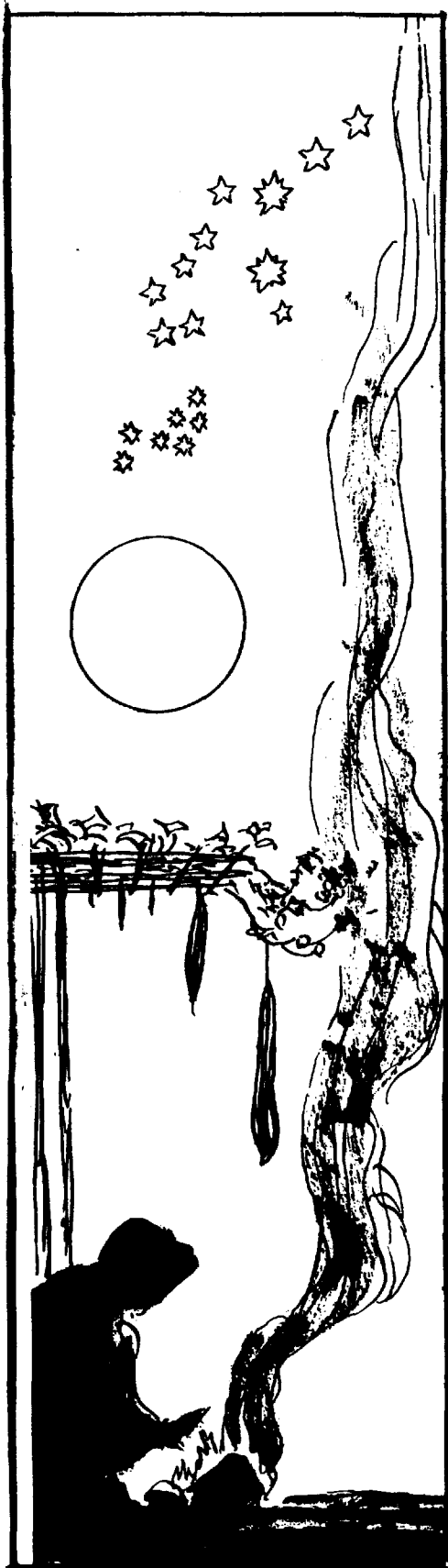
~~TOP SECRET UMBRA~~

I left the 330th in December when the offensive was all but over. There were still occasional attacks by fire (one several weeks after I left destroyed my work table), but reporting was dominated by indications of withdrawal and regrouping. The night before I left, there was to have been a farewell party, but it had to be replaced by a quick get-together in the operations quonset. Everybody was too busy to take time out. After that, I knew the 330th would never change.

\*\*\*\*

*The Burmese believe that the possession of a stake which has been driven into the ground about to be built upon, wards off danger from the possessor; when such ground has been consecrated there is a strenuous effort made to secure these stakes. If one is suspended from the roof of a dwelling, they believe it will keep away bugs. They are also supposed to avert dangers such as fires, etc. Burmese doctors mix the scrapings of these stakes with their medicines as a preventative against evil spirits.*

\*\*\*\*



တန်ဆောင်မုန်းလပြည့်

ငွေစန်းရယ်တဲ့ပုဏ္ဏမိ၊  
ရွှေကျီးညိုတာရာနဲ့၊ ကြတ္တိကာယှဉ်ပြိုင်လျှမ်း  
တယ်၊ ချမ်းစရာသီ။

လှူကထိန် ခါတော်ပွဲနဲ့၊ ခဝဲပွင့် ဝါစီစီ၊  
သာကြည်လဲမြူရှင်း။

လ-တန်ဆောင်မှာ၊ ကြပြောင်ပြောင် အသေ  
တင်ပါဘိ၊ ရွှေမြင့်မိုရ်ဝါထိန်ထိန်နဲ့၊  
ခါအချိန်မြောက်လေသွေးတယ်၊ ငေးတဲ့ငွေနှင်း။

ဦးပျံးချို

**The Month of Tazaungmon**

**By U Pyone Cho**

The Moon has now wax'd full,  
The Scorpio and the Kartikka both  
for radiance vie,  
And the first spell of cold is felt ;  
Ahus, kahteins fill the month,  
And the Luffa too has blossom'd,  
Gay, exuberant :

The month of Tazaungmon is truly  
magnificent,  
Glittering like the golden Meru :  
The north winds have begun to blow  
Ushering in the silvery mist,  
And chilly is the weather.

**Tazaungmon = November.**

**Kartikka = A lunar asterism.**

**Ahus = Religious offerings.**

**Kahteins = Festivals marking charitable  
deeds, when robes are offered  
to the sangha.**

**Translated by Kenneth Ba Sein.**



~~TOP SECRET UMBRA~~THE CINCPAC INTELLIGENCE COORDINATION GROUP -  
AN INTELLIGENCE MANAGEMENT CONCEPT

by Walter D. Abbott, Jr., B614

In the world of statistical analysis concerning the war in South Vietnam, the subject of infiltration has long been an enigmatic variable, used in a myriad of manners to prove either imminent success or pending disaster, as the caprice and motivation of the moment dictate. Although a network of manual Morse stations obviously supporting the North Vietnamese infiltration routes through Laos to South Vietnam was isolated in SIGINT as early as 1963, messages passed on this network were not textually exploitable, and it was left to the imaginative speculation of the intelligence community to decide whether message volumes related to infiltration flow and to determine what, if anything, was physically passing through the infiltration system. Until mid-1967, the only determinant of personnel infiltration into South Vietnam rested with MACV through interrogations of POWs and Chieu Hois and evaluation of captured documents. This process, tedious at best, resulted in statistical information on personnel infiltration long after the fact (generally nine to twelve months were required to ascertain even partial infiltration for any given period); this contributed only historically to the command decisions regarding pursuit of the war.

It was known that the North Vietnamese used low-VHF, R100 series equipments in their Air and Air Defense communications, and these communications were being intercepted on a continuing basis primarily through COMBAT APPLE and COMMANDO LANCE support of U.S. airstrike activity. It was also known that there were messages being passed over these same frequencies which were not Air and Air Defense messages, but it was not until the Fall of 1967 that NSA had enough volume of non-Air/Air Defense material to determine the importance of these intercepts.

[REDACTED]

This traffic was identified as representing communications between elements of the North Vietnamese General Directorate of Rear Services (GDRS), the organization responsible for supplying men and materials to South Vietnam.

EO 3.3(h) (3)  
PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Particularly significant in this exploitation of GDRS communications was the information appearing on personnel infiltration. As the picture developed, a complex structure devoted to the transportation of manpower emerged, marked by small rest stations, approximately one walking day apart, in charge of caring for groups of traveling troops as they passed through each area. Moreover, each station was apparently tasked with providing a daily report to its superiors on the status of the travelers; these reports showed how vast and organized the infiltration process really was. Every infiltration "group" was assigned a designator, first in a three-digit and later in a four-digit series; generally consisted of approximately 570 men; and was destined for a specific location within South Vietnam, a destination which could be determined, at least in part, by the initial digit of the group's designator.

This exploitation of GDRS communications generated several immediate problems for user and producer alike. Based on the number of personnel reported in these messages as heading south, it became painfully apparent that the accepted MACV infiltration estimates were extremely conservative and did not reflect a true force threat in the war zone. As intercept techniques improved, and the SIGINT production community geared up to handle this information on a continuing, timely basis, the mass of data being generated far exceeded the handling capabilities of individual intelligence shops. The approach to the problem was rapidly degenerating into an exercise in comparative bookkeeping on group numbers and strength figures, without an understanding of the capabilities, intentions or vulnerabilities of the GDRS system.

Under the reverse concept of Parkinson's Law, so often applied to any problem with substance and meaning, the immediate management reaction is that additional personnel are required to deal with this data. By early 1968, this lament echoed throughout the intelligence community in regard to GDRS, and more than one command took the approach that while the information was valuable, it could not be addressed until sufficient people were acquired to properly massage and file the material being received. For once, however, this approach was summarily dismissed. CINCPAC, taking the position that as

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

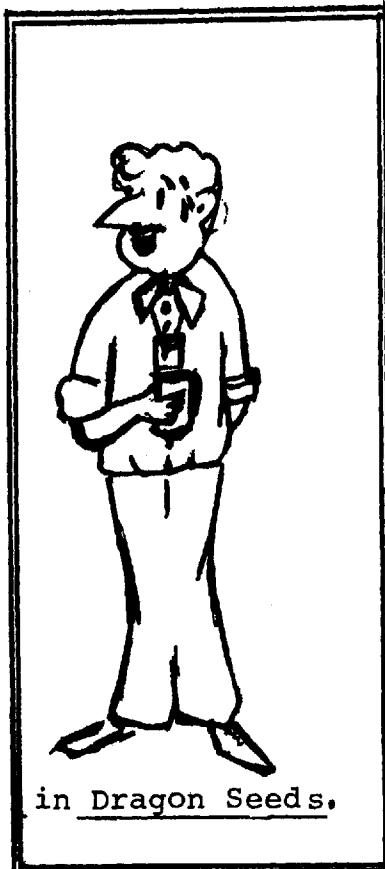
overall theater commander, it was his responsibility to apprise MACV of imminent threat; and realizing that intelligence-oriented manpower resources were already stretched paper-thin, decided that a) CINCPAC was the logical point at which all GDRS information should be amassed and consolidated; and b) that this amassment and consolidation would have to be done within the parameters of existing personnel resources. In April 1968 the Intelligence Coordination Group was conceived, chartered and tasked.

CINCPAC divided the GDRS problem into two major subject areas. In general terms these areas were tactical/strategic and political/estimative. Under these headings, the principal intelligence officers from every major command on Oahu (PACAF, PACFLT, USARPAC, and FMFPAC) as

well as Hq NSAPAC (representing NSA and the SIGINT community) were convened and received their tasking. CINCPAC's approach to this tasking was simple and direct -- task each command within its area of primary interest, put an end to repetitive duplication, and therein effectively apply existing capabilities and resources to an over-all attack on the problem. Under this concept, PACAF and PACFLT, as the two commands with airstrike responsibility, were to perform correlative analysis on translations, photo intelligence, OPREP-4 information and any other available data to develop GDRS facility locations for targeting purposes. USARPAC was to determine the GDRS order-of-battle and provide a correlation between U.S. and North Vietnamese designations for various routes primarily used in the infiltration process. FMFPAC, through the 1st Radio Battalion, was tasked with developing and maintaining a file on personalities associated with infiltration. NSAPAC undertook the job of communicating to the SIGINT community the needs and requirements of the ICG for SIGINT data, as



Happiness is an article ...



in Dragon Seeds.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

well as functioning in a liaison capacity as the focal point for all queries regarding the SIGINT posture on the problem. CINCPAC retained the tasks of providing a monthly infiltration estimate, developing a machine capability for storage and rapid retrieval of infiltration data, and over-all supervision of the ICG.

As could be expected, the ICG concept was greeted with varying degrees of enthusiasm by the tasked participants. Natural suspicion of both the motives and motivations of CINCPAC arose, along with fear that command prerogatives and production techniques were being jeopardized if not actually usurped and exploited. The result was an extended period of fermentation with only marginal output. Internal dissatisfaction with the ICG developed, and at one point, the whole concept was almost abandoned. But breakthroughs did emerge. USARPAC compiled a basic order-of-battle study on group activities, which, with some modification, provided the foundation for the initial CINCPAC ICG publication. CINCPACFLT, through the efforts of FICPACFAC, then provided the first comprehensive study on suspect GDRS facility locations. Using these as a sounding board, other efforts were initiated and the operation began to jell. Both DIA and MACV, in conference with CINCPAC, agreed to accept the CINCPAC estimate as the authoritative statement on infiltration, allowing for reasonable exchange between analysis on any point of dispute which might arise. CIA, through their DODPRO representative, modified certain of their operations to attempt to acquire more information which could be used in assessing infiltration. MACV became an active participant in the ICG per se, and accepted tasking for input of collateral data to be married with other inputs available to the ICG. NSA provided technical material to assist the ICG analysts in a better understanding of both the possibilities and limitations of SIGINT information. In general, after several turbulent months, the ICG started to function as conceived, and has continued to function even today.

Two points need to be addressed in this regard. While it is an easy trap to fall into, CINCPAC did not envision and earnestly avoided creation of the impression that the definitive word on infiltration could come only from CINCPAC. The effort was intended as a collective venture, with any and

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

all opinions considered as contributory to an over-all understanding of the problem. In furthering this approach, a dialog among all concerned analysts was initiated under the heading of an "ICG analytic exchange," so that every party involved in the infiltration problem was at once free to air his views and also privy to the opinions of others. Over the months, as suspicions gradually diminished, these dialogues were openly expanded and have materially contributed to ICG conclusions on the problem without binding the originators either to command opinion or channel violation. Further, although the problem at hand is still the North Vietnamese infiltration problem, the mechanism of the ICG can be modified, expanded or otherwise adjusted to deal with any intelligence situation requiring maximum utilization of limited resources against a particular target or subject. Through careful direction and judicious integrity the ICG will continue to exist long after the infiltration problem has vanished and will apply its burgeoning expertise to other areas of common interest.

This is not intended to be an eulogistic endorsement of the ICG. The ICG admittedly has had and continues to have shortcomings. But it has proven that dedicated application of available resources can oftentimes be more effective than acquisition of new ones; that with proper management, the intelligence community can function as an integrated whole rather than as many parallel, internally-competitive parts; and that through such an effort, all agencies and commands can reap a collective, beneficial harvest through full participation, understanding and acceptance of the principals underlying all-source intelligence. A hard-fought lesson, it merits study for future emulation at all levels.

\*\*\*\*

*"To the degree that people believe their solutions are the only ones, they begin to limit themselves and their futures."*

~~TOP SECRET UMBRA~~

CRYPTO-SCRAMBLE

By Richard Atkinson

Unscramble each of the five numbered crypto-scrambles, placing one letter in each space, to form five words or names, each of which fits the definition to its right.

1. A Y E K I N G P E T E R  
\_ \_ \_ \_ O \_ O \_ \_ \_ \_

Orders components.

2. F R A I L P A Y  
\_ \_ \_ \_ O \_ O \_

System statistically diagnosed by the digraphic I. C.

3. B U S T B Y  
\_ \_ \_ O \_ \_

RYE program which does the remainder test.

4. E N D C O N I C I C E  
O \_ \_ \_ \_ \_ \_ O \_ \_

A hit.

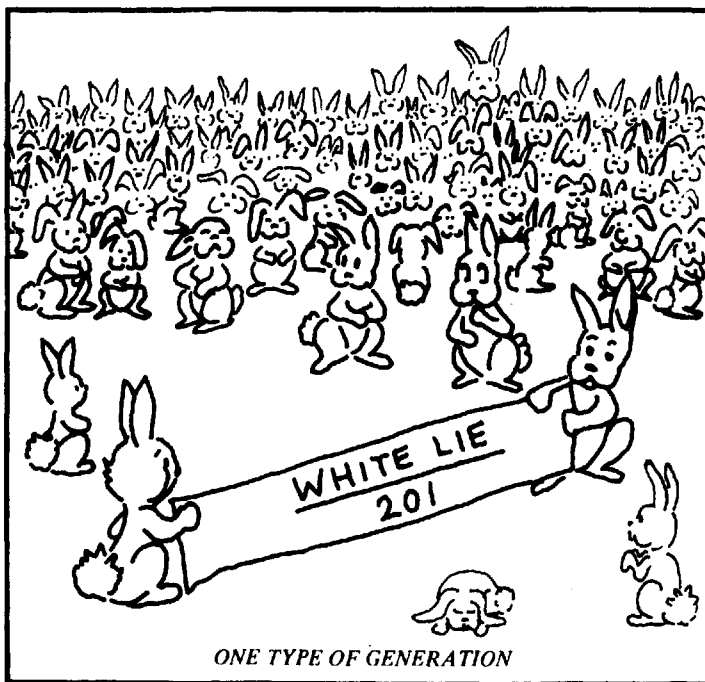
5. C O D E I R I P  
\_ \_ \_ \_ O \_ \_ O

Cyclic.

Now arrange the circled letters to form the cryptoanswer suggested by the cartoon at the right.

Print CRYPTOANSWER here.

\_\_\_\_\_



U 7 Answer on page 47.

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605AG-22: WHERE DO WE GO NOW?

by Phil Remsberg, B41

As a crossbreed or hybrid analyst (traffic analysis and data systems), I have been directly involved with the planning, testing and operational use of the AG-22 system over the past 4 years and have an observation, a question and a proposal.

First the observation. From the B Group traffic analysis standpoint, two major milestones have passed in the preceding 6 months. The first milestone was the turn-on of all AG-22 equipped intercept positions directed at People's Republic of China (PRC) targets, and the operational use of the daily processing cycle (GAPS, NOOSENECK, et al.) at NSA in April 1972. Why is this significant? The primary significance of this milestone is that for the first time the B Group traffic analyst has become almost solely dependent on machine processing to supply him with the "staff of life," raw traffic (that is, PONETO listings). If the AG-22 system becomes fully operational, the analyst will no longer do traffic analysis from the "blue's and green's" nor choose whether to get and use machine aids. (Now, however, if someone pulls the plug in C Group, the B Group traffic analyst is in real trouble!) Of equal importance, but perhaps unrecognized, is the fact that for the first time almost all of B Group's many and varied target activities are processed together at one time, in one place, and in one format - even though it may only be for 24 hours after intercept. This new method of processing intercept may not seem significant, but as an analyst steeped in the  problem and the long-range, cross service callsign, frequency and practice traffic problems, I believe this new method is a "great leap forward." Anyone who, in an attempt to process data, has had to deal with two or more formats and such statements as "That tape is being used to run my monthly now, maybe next week," will appreciate just how much of a forward step this method really is. The many new approaches opened up to an analyst when he has a complete data base with which to work are amazing; for example, the phenomenal success of the reidentification programs in NOOSENECK explained in DRAGON SEEDS, Vol 1, #2.

The second milestone was reached on 22 September 1972 when virtually the entire PRC data base went on-line for 14 days (building to an eventual 6 months) to the COPE terminal. The fantastic possibilities inherent for TA mechanization in this

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

development are only now being explored.

Within five years, I think we will look back on these two historic events and say that traffic analysis in B Group was revolutionalized for the better in the "Summer of '72." Unfortunately, I have also observed that, from the desk analyst all the way to top management, an attitude exists that precludes the all-out effort necessary to take advantage of all TA mechanization possibilities. A revolution has occurred, the "king" has been displaced, and very few seem to be taking advantage of the opportunity to change the order of the TA world. That statement leads me to my question.

If my premise that a revolution has occurred is correct, then why is B Group high-level management not actively pursuing a program to consolidate and control all the various old machine programs and to initiate, coordinate, evaluate and develop the new ones? Now is the best time to exercise some strong authority to maximize the machine resources available to B Group in order to take advantage of both the new and sophisticated machines and the new TA mechanization possibilities. We can no longer afford the narrow, provincial view of every area doing "its own thing" with machines. Consolidation sometimes has its own rewards which in this case would be manifested by more machine time, more programmer time, better TA support, elimination of duplicate processing, etc.

What am I proposing? That a group consisting of B Group traffic analysts, data systems analysts, and C Group programming support personnel be formed. That this group be given the authority to chart systematically the complete data-flow of B Group processing from both the machine and the analytic standpoint. That each machine job or process be evaluated as to benefit derived and the input, processing and output accomplished in relation to all other B Group jobs or processes. That an effort be made to make each analyst aware of what is available to him in the machine area and what his responsibilities and contributions are and why. And finally to streamline, consolidate and manage a complete B Group processing system designed to serve the best interests of the final user, the analyst. There is a crying need, why can't it be heard?

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~THE DEVELOPMENT OF A COMINT TRANSLATION COURSE FOR  
VIETNAMESE LINGUISTS

by Jack R. Sharretts, B6

Like supervisors in other language areas in the Agency, those associated with the Vietnamese problem have long discussed the idea of developing a translation course designed to facilitate the transition from the types of texts presented in basic translation courses at the NCSch to the more esoteric material encountered by the COMINT translator on the job. A number of objectives were gradually defined through informal discussions on this subject among various individuals, and early this summer a preliminary modus operandi and course outline were circulated among several of the senior linguists for their comments and suggestions.

It was generally agreed that the course should employ current traffic for the translation exercises as much as possible. In addition, the course was broken into blocs and several senior linguists-supervisors were designated as instructors for these blocs and given the responsibility for assembling material for them. The class sessions are scheduled to be held twice weekly in the afternoons in a conference room within B6. This assures that no one senior linguist will be away from operations for an extended period, that processing of the "morning mail" will not be affected, and that the "student body" will also be away from their sections for a minimum amount of time. Once those ground rules were established, the problem of course content was addressed.

It was the consensus that a COMINT course should deal with two major problems encountered by the new COMINT translator. Of course, the first concern was with "purely linguistic" matters such as specialized vocabulary, telegraphic spelling systems, "telegraphic style," corrupt texts, unrecovered code groups, ad infinitum. The other aspect, considered equally important, was what we shall call the "background" or "intelligence setting" which the COMINT translator must thoroughly understand before he can operate effectively. For purposes of COMINT translation, a great deal of target orientation is required in order to place the messages in the proper context for the most accurate translation. This premise led to a course outline which was devoted about equally to lectures on various intelligence aspects of the

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Vietnamese Communist problem and translation exercises. For instance, the importance of understanding North Vietnam's governmental structure and operations to the translator of messages from the NVN Civil Network can be demonstrated by showing how garbled message addresses can be reconstructed when the translator knows with whom the Ministry of Communications and Transportations usually communicates in Son La Province. Similarly, the applications of T/A and C/A in identifying military correspondents and placing their messages in the context of their operations will be discussed at length.

In addition to stressing the "intelligence setting" so strongly, perhaps the most significant innovation made in developing this course is that of breaking it into blocs paralleling the present operational organization's division of the problem and designating the senior linguist(s) supervising translation in these elements as instructors for the blocs covering their portion of the problem. Thus, the instructors of the various blocs are the most skilled and knowledgeable people available and the most acquainted with current developments in their areas.

The course as it is presently structured runs 20 weeks (two 3 1/2 hour sessions per week). It is not designed to turn out "experts" on any one portion of the problem, but rather to familiarize the apprentice or journeyman translator with the art of COMINT translation as it is practiced in B6. Since no formal course can possibly prepare a budding COMINT translator to handle all the problems and avoid all the pitfalls encountered on the job, this course will stress recognition of types of problems and methods of attack. Ultimately, this training should benefit the individual translator by making him more effective in his present assignment and improving his ability to shift from one area of the problem to another with a minimum of transitional training. This versatility will directly benefit the organization, since linguistic resources can be shifted more quickly and smoothly when it is necessary.

The present course outline will no doubt be modified somewhat as operational requirements change, but the pilot course will cover subjects in the following order:

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

Introduction - Lecture on the use of working aids, dictionaries, and other reference material...a brief discussion of the SIGINT Publication Manual.

Bloc 1 - North Vietnamese governmental organization and standardized nomenclature of the NVN governmental organs...NVN civil, diplomatic, and shipping communications...translation exercises using sample texts from these communications.

Bloc 2 - Provisional Revolutionary Government, its organization, communications...special terminology, message formats...translation exercises...

Bloc 3 - North Vietnamese military organization and operations...Ministry of Defense and the High Command...background and history...equipment/weaponry designators, divisional T/O...translation exercises from open source texts on military subjects...

Bloc 4 - Linguistic applications in "low grade" cryptanalysis...word patterns, stereotype beginnings and endings...C/A working aids...briefing on processing in B63 and tour of the operational spaces...

Bloc 5 - North Vietnamese tactical military traffic...translation exercises using current tactical traffic from Laos, the DMZ and I Corps...discussion of problems in dealing with this material...geography, O/B, tactics...

Bloc 6 - North Vietnamese Naval and Air-Air Defense Command lectures on organization/equipment/weapons...cryptosystems employed, message formats...

Bloc 7 - South Vietnamese Communist military traffic...VC military organization...dialectical variations and other linguistic peculiarities...translation exercises.

Bloc 8 - The North Vietnamese General Directorate of Rear Services...history, development, organization, and current operations...specialized terminology, message formats...translation exercises.

Bloc 9 - North Vietnamese multichannel communications...equipment capabilities and communications procedures...special terminology...translation exercises using transcripts of NVN military and civilian multichannel material.

~~TOP SECRET UMBRA~~

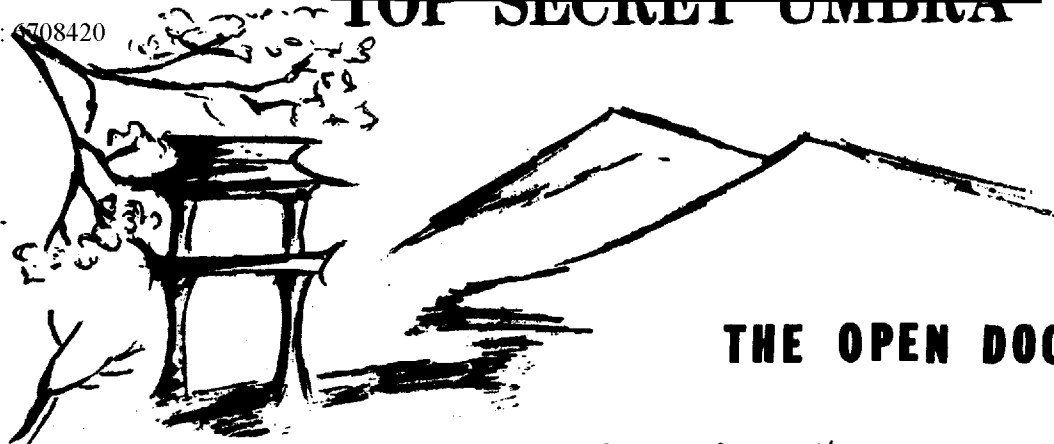
~~TOP SECRET UMBRA~~TRANSPOSITION:

*The Basic Cryptologic Glossary* defines transposition as "a cipher in which the elements of plain text undergo some change in their relative positions without a change in their identities." The following is an example of this form of encipherment. Can you solve it?

N O L I T	E E L U R	N B L U E	I H H X C	A T R H H
A D C D E	E O D N D	R N D O T	I E H C P	X A R D U
P S Y Y A	B A X H W	E F O I A	I B D R H	N B K E M
O A I R R	N V R N F	A E N H U	O E T I T	N O L X D
N T J A D	V T U S E	V R D N I	N N S O A	T O A N N
R S X U I	O M E S T	R Y N H Y	O E I S N	F N N X T
D H E S D	M H S L F	G O U R C	E E E C O	H S R A E
O R N O S	S A I R X	L E H I A	A E E N W	O S R I E
B D S T C	N I T U R	N A A B U	L E S O S	I F P E A
H M A N N	D P A E I	T T M E R	U U X G R	E A S F F
L W H X E	T N G B R	H R T E I	T X A E S	N R E E H
I D I T L	O H O D E	T W T O F	U D T X N	R O I X P
T E F U R	S O H I E	I E R S O	T H E O E	E G N N H
T N U X D	B N O E S	B T U D F	X S M A S	E T S T D
H B F E S	N O I R D	E T H N S	S U E D I	E S A N S
L T U V M	F C E V R	F R U S F	O T T M G	A S E E A
I A E A E	S L A T R	E W O H F	U N W I H	E D A N S
D E L U E	I D E T B	E W T S I	E N G O F	L A N I I
I E N D T	O R N H N	N R C X M	T E P T A	N R E A W
A E O U N	R H E R O	G H O O O	0 0 0 1 3	0 0 4 8 7

Answer on page 46 .

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

## THE OPEN DOOR

*We seek to be companions along the way.  
 The lantern which we carry is not ours.  
 The spirit which we share is contagious thought;  
 The knowledge which we gain, an illuminating torch.  
 And all who seek may perceive and learn.*

*-The Concept of Dragon Seeds*

### DON'T SAY MUSSO--Say USSID (There Is a BIG Difference)

by Louis C. Grant, ADPSD

Someone once said, "The field thinks NSA is crazy and they have the papers to prove it." He may be right! We don't always do a very good job of getting good instructions to the field. Yet those instructions can make or break the Director's control of U.S. SIGINT operations. The need to improve both the instructions and the mechanism for getting them out is why the Director set up the United States Signal Intelligence Directives (USSID) System.

Before USSID, we had 12 years of MUSSO with its some 600 TECHINS, OPINS, OPDOCs, and TECHDOCs. MUSSO was good in that it gave the Director a mechanism for exercising control, and instructions were getting out. But MUSSO lacked central direction, it was over-engineered, and it bogged down in its own procedures. The Inspector General took a look at the problem in 1969 and found that MUSSO was a mess. At best, it had become more traditional than functional. He stressed the lack of central direction, saying: "One can only surmise how much better the exercise of operational and technical control would be, and therefore how much better the product, if the established means for exercising them were well managed."

The need for central direction is why the USSID system must concern all of the means for getting instructions to the field: formal messages, hard-copy USSID and OPSCOMM. That is also why only USSID or issuances authorized in USSID may be used to direct SIGINT operations.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The ADP runs the USSID system because he is the Director's agent for day-to-day control of SIGINT operations. An element of the ADP's personal staff, ADPSD, manages the system procedures for him, reviews and issues the directives, and makes sure that he gets in on USSID decisions. This set-up has gone a long way toward wiping out the "my document" syndrome. Elements get into the act depending upon the degree of their responsibility or what they can contribute. But no element has absolute authority over a document. The ADP (or the DIRNSA) owns them all.

As we review the draft USSID, we are making good progress with many of the MUSSO problems like textual style, clarity, presentation, etc. But there are a couple of deep-rooted problems that are tough to get at. One is a lack of understanding about what the field needs. The other is what commercial contest writers call "aptness of thought."

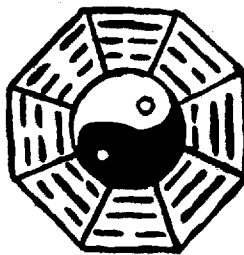
Our managers and action people are close enough to the problems to know the issues and answers. As a result, they often don't push for really good instructions. We have to judge our instructions in terms of what they mean to the guy in the field. First, our instructions are his marching orders. Second, they are his guidance. Third, they are all he has. He must do what we tell him, the way we tell him, without a crew of on-call experts around to interpret for him. We must say what we mean, do what we say, and if we change our minds, we must change our instructions.

"Aptness of thought" translates to "does this make sense?" Before we convert a MUSSO document to a USSID, we must take a hard look at what it does to make sure that the directive provides the best way to do the task; it doesn't conflict with other directives; the task should be done in the field; and the field has the resources to do the job. We must not continue, or issue, directives unless they are needed. And we must get the tired, outdated ones off the street. Although there is no "USSID of the MONTH" Award, the quicker we do this, the better for the field. ADPSD is available to you. If you have any doubts, or questions, talk it over with us before you spend a lot of time writing something. We have the people and the experience that can make your job easier.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

USSID is indeed more than a new name for MUSSO. USSID is a better mechanism for getting good instructions to the field. But you can bet that it will stay that way only as long as we all give it our attention and support. We made "MUSSO a mess" over the past 10 years; let's not use the next 10 to make "USSID useless."



#### The Eight Diagrams and Symbol of Creation

These eight combinations of straight lines are said to have been evolved from the markings on the shell of a tortoise by the legendary Emperor, Tu Hsi, 2852 B.C.

Wen Wang, 1231-1135 B.C., founder of the Chow Dynasty, appended certain explanations to each. His son, Chou Kung, added still more and they became known as the "Canon of Changes," the most venerated and least understood of the Chinese Classics. These Eight Diagrams were the basis of a system of an ancient philosophy and are supposed to contain the elements of Metaphysical knowledge and the clue to the secrets of creation.

The Yang and the Yin, the symbol of Creation pictured in the center, are the positive and negative principles of Universal life. These two, male and female principles of nature, constitute the eternal principles of Heaven and Earth and are the legendary origin of all things human and divine.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605MACHINE-AIDED TRANSLATION

by Normal Wild, B03

*This, the last of Mr. Wild's three articles on machine-aided translation, examines the use of machine look-up in NSA, past and present. It may stimulate some thinking about the advisability of using this modern tool more widely in the language field.*

Automatic Look-up

One of the earliest uses of automatic look-up in NSA was the printing of bilingual vertical message prints (VMP) of Japanese military code traffic during the Second World War. For example, if the group 1234 represented BAKUDAN ("bomb"), the code recovery submitted for the VMP was "BAKUDAN//BOMB." The expense of preparing a few more letters for the entry was trivial, and no new techniques were required. Isolation of the lexical entry was accomplished by the code group itself. It was of course possible, if unlikely, that BAKU was sometimes part of a preceding word and DAN part of a following one. The two extremes were the code group for an entire sentence, which could be rendered in English with minimal loss even if the Japanese were omitted, and the code group for a Japanese syllable, where the English equivalent might do more harm than good.

Unquestionably, the bilingual code group was a great help to the crash-trained scanners and translators who worked under a thinly stretched group of experienced linguists. Their work was better and faster than it would otherwise have been and benefitted from the fact that the English equivalent could be used to resolve ambiguities of the Roman spelling, printout in Japanese script not being practical at that time. To some translators, that fringe benefit constituted the sole value of the English.

Since WWII, bilingual code groups have been little used. Batches of Laotian Communist political traffic [redacted] were so processed with some benefit. Only code groups for words and phrases were put into English since it seemed over-ambitious to fit together syllabic

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

streams and to find equivalents on a dictionary tape. The cool reception given to the bilingual code group can arise either from the lack of neat lexical units in the codes--many Asian codes have a high percentage of syllabic values from which poly-syllabic words are composed--or from fear that the English equivalent will be unnecessary to the experienced linguist and a harmful crutch to the inexperienced. But it would be a bit much to say that bilingual code values would not be useful anywhere in NSA.

Bilingual code groups carry a fringe benefit--economy in data preparation under certain conditions. When an entire codebook in encode order is obtained after being abandoned by enemy troops, a decode bank for VMP can be prepared by matching the code groups to the file-maintenance numbers of a dictionary tape and picking up the plain value in the language plus, at no extra cost, its English equivalent. It should be faster and more accurate to input a several-digit file-maintenance number than to input the plaintext value, especially if the native script requires a cumbersome conventional coding. Should such a program be established, the senior linguist in an area would control it. He might assign English values for the sole purpose of indicating standardized translations. It is well to consider that, if bilingual code groups might be useful some time under some circumstances, now is the time to get them ready.

The only place in NSA where full texts are matched against a dictionary bank--in principle, giving English for all the words in the order of their appearance in the text--is the Chinese Communist (PRC) civil problem. Very possibly, the balance of pro and con (as listed in the second article of this series) is more favorable on that problem than elsewhere. There are huge volumes of material which would be machine-processed in any case, mainly for categorization and distribution. The additional cost of finding and printing an English equivalent is fairly small. Much of the material is used for long-term studies, so the processing delays are tolerable. The average Chinese linguist on the job is slowed down considerably by having to thumb the dictionary. He is also troubled by "false friends" (words which do not mean what he thinks they do), by problems in breaking the stream of syllables into words, and by the need to memorize or to look up the telegraphic code for lack of a printout in Chinese script.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The Chinese linguist probably gains somewhat more from an automatic look-up than do workers in other languages. The base form of a Chinese word is not subject to inflection, so there is no problem of removing inflections to find the base. The stream of Chinese characters is represented in plain text by a stream of four-digit numbers, occasionally interrupted by a foreign word or by digits in parenthesis used for their true numerical value, making it "neat" for machine handling. On the other hand, the stream of groups has no indication of word separation and sometimes none of clause and sentence separation, and there is little in the "shape" of the Chinese characters to help. There has to be a program to find words in the stream, and that program would involve some trial and error. Groups of syllables looked up might not turn out to be the true word divisions of the text, and even if they were, the true word-division may not be in the dictionary and a "no match" would ensue in either case.

The PRC Civil program has been used on two unclassified books as an experiment and as a training aid. Since authorized translations of the books are available, a translator can try for himself to see how helpful the program is, and the person who knows no Chinese can see how well he understood the text with the machine version alone.

Much the same program would be applicable to other languages such as Vietnamese which are written or transmitted in syllabic units and have little or no inflection. Thai and Lao are, loosely speaking, monosyllabic like Chinese, but many words of Indic origin are quite long and would not be caught by a four-syllable cut. Korean is poly-syllabic, but it is conventionally written one syllable at a time; the noun has no inflection, but the verb is lavishly inflected. The verb inflection does not always change the form of the verb stem which might still be caught. Cambodian is poly-syllabic but not inflected; if the language is input one syllable at a time, it could probably be handled by such a program. In fact, given a syllabic stream, "the machine wouldn't know the difference," whatever language is used.

There would be some insurance value in a bilingual code program for rare languages, such as some of the minority languages of China, for which there is little or no demand at present. In an emergency, a good linguist would be able to do something with a text, given the printout and some hasty study of grammar.

~~TOP SECRET UMBRA~~



Automatic "on-call" dictionaries have been used in NSA for Spanish (CAMINO), Vietnamese (RICEBOWL), and French (FRANCO-PHONEGLOS). Essentially, the user types in a word or phrase and gets back a definition, either printed out or displayed on a screen. Dictionaries, being merely a particular type of information file, may have to share time with other files, but the automatic dictionary has several advantages over a printed book. Chief among them is that the file can be updated rapidly and often, while a desk dictionary is normally updated once in several years at best. Other advantages are speed in some cases (it may be possible to put in a number of words at a time and get a rapid printout of all the definitions), and various fringe benefits from the availability of the data for machine manipulation. The desk dictionary, however, is always available (no time-sharing, down-time, and rewriting problems) and requires no typing for input. Possibly the best combination is a printed dictionary for well established information and a machine dictionary as a live file to use between editions and for ephemeral information as well as for the fringe benefits.

Responses to CAMINO and RICEBOWL, as machine systems, have been mixed. To many people, they are only a way of getting a hard-copy dictionary--which is by no means a small benefit. Their usefulness as a degarbling and recovery aid depends on whether conditions are optimal or real-life. The quality of the file and its timeliness depend on the people who contribute to and manage it. Of course, the same is true of a card file in a cardboard box; it is easy for a passerby to take cards out of a box and lose them or to write anonymous information on a card. The computer dictionary in some ways encourages good management. Not only is access to the file controlled, but several different people can refer to it simultaneously.

If computer dictionary files do not exist throughout NSA, it may be that they were considered and a thoughtful decision made that they were unnecessary. But maybe not.

\*\*\*\*

*"Those who have free seats, hiss first."*  
--- Chinese proverb

~~TOP SECRET UMBRA~~THE WADE-GILES SYSTEM

by E. Leigh Sawyer, B02

(Author's note: The demands of time have permitted little opportunity to check my memory against primary source materials lending themselves to glossological substantiations. Minor aberrations, it is hoped, may be found excusable.)

為無為

For the p'erson who has had little exp'perience with the Ch'inese lankuache, the p'ronouncing of p'lace names, p'eo'p'le's names, art'ifak't's, and even the inkretient's of Monkolian parpek'ue is often k'onfusing. An unterst'anting of at least Wate Chile's ap'ost'rophic usache aft'er cert'ain k'onsonant's chust might enaple one t'o atchust himself t'o this esot'eric linkuist'ic area. A little pak'ground on Wate Chiles might pe in orter. Wate Chiles was porn in Ch'ik'ako, and lat'er moved to Cheorchia. At that t'ime, his mother atvised him, "You ought t'o invent something. Why ton't you ko t'o Ch'ina, Wate, and invent the Wate Chiles syst'em?" He said, "Poy oh poy, mom, puy me a t'ik'et and I will t'ake the first poat leaving p'ort." So he t'ook off for K'athay. His letters t'o his mother reflek't the choy he felt in t'raveling from p'lace to p'lace. He mate reference t'o the many intichenous t'ype nat'ives he had pump'ed int'o, and the cheokraphik'al ottit'ies he had seen. In any k'ase, as may be kauched py it's witesp'read usache t'otay, Wate invent'ed his syst'em, and it is seen on map's and all k'inds of swell st'uff all over the p'lace.

On the pasis of the k'arefully kathered tat'a p'rovided apove, one k'an easily tecite how t'o p'ronounce that p'art of a Ch'inese p'lace name that has an ap'ost'rophe in it, and one which toesn't - also p'rop'er names (poys or kirls) and telek't'aple Ch'inese tishes such as K'ant'onese st'yle pean k'urd.

~~TOP SECRET UMBRA~~

T/A-MATH SYMPOSIUM REVIEWED

by David J. Tiren, B61

The September 1972 Dragon Seeds noted B participation in a symposium on Mathematics and Traffic Analysis. David Tiren, B6, attended the symposium and prepared his comments in a stream-of-consciousness format. Because of the B interest in this subject, he offered his remarks to Dragon Seeds. He reminds us that they are subjective and do not cover all presentations, but are some of the highlights of the symposium as he remembers them.

"I attended the T/A and Math Symposium held by Pl at FANX II on 24 and 25 May 1972. A hardcopy transcript will be available ultimately; however, I thought some quick notes and observations might be useful. I won't include all the speakers or even all the ideas of those I will use, but just some of the highlights as I remember them.

Robert Prestel spoke of D7 and some of its operations. As an example, he used a system for choosing an intercept site against a given target, while trying to predict what frequency and schedules the target might use. Over-simplified, it goes like this. Using wave propagation data available through open and other sources, an estimate of the optimum combination of receiving frequency (perhaps in increments of a tenth of a megahertz) and a time (24 hourly increments) is made for a given target station. All the combinations which meet a certain threshold of probability (say 80%) are noted. The same thing is done for the other end of the target link. The intersection of the two sets of data provides all the probable frequency/time pairs the target link will use. The next step is to estimate these probabilities for each potential intercept site. The site whose set of combinations (again, over the same threshold) has the greatest intersection with the set for the target link is the candidate for the task of intercepting the link. The last step in the process is setting up a program for systematic search, the specifics being based on the technical data provided.

Foster Slade, B3, gave some practical examples of a desk analyst employing simple arithmetic to recover aircraft type designators using times reflected in navigational air traffic in conjunction with known airfields. If a given designator, known to represent an aircraft type, is observed consistently in the

~~TOP SECRET UMBRA~~

context of the amount of time it takes to go a known distance (i.e., we know its speed capability), then it can be only this or that type of aircraft. Once ample data is available, all designators should be recovered. Conversely, if we have all designators but certain airfield cover numbers are unrecovered, we can use the same kind of math to compute the distance from known points, using known speeds/times. If computing the distances gives us a point on the map which is near an airfield, we have made a recovery. Basic, but it is an application of match by an analyst.

Ken Cohen, B45, talked about recovery of three-digit

[redacted] demonstrated interesting uses of computers to solve topological problems. One of them involved plotting some towns in England, Wales and Scotland. The computer was given a list of the towns and the distances between all pairs of towns, (much like mileage charts on our road maps). The computer then plotted all the relative locations. Since the towns were chosen wisely, the resultant dots on the map formed a rough outline of the island of Great Britain.

A second application was shown by the use of counties. A list of the counties of Great Britain, plus the number and name of the counties on which each county abutted was given. The computer then printed out the name of each county in its relative position. The result was a little distorted because of the great variances in size among the counties. When the technique was applied to the departments of France, the results were phenomenal, as those departments are similar in size.

Caterino Garofalo, P14.

More about Gary

later.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Richard Atkinson, P12/E13, appeared in a film produced by the school. The film drew analogies between the Delta Index of Coincidence (I.C.) and baseball batting averages. It was the clearest explanation of I.C. and its uses I have ever seen. Four Stars, rated G.

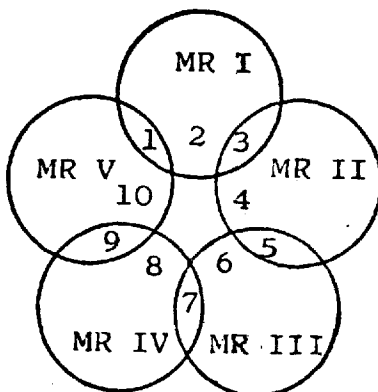
Floyd Taylor, A75, spoke about spherical geometry and its uses in plotting from radar information. Questions from the audience about "Why go through all this geometry when the TALL KING radar is line-of-sight gear?" left this subject sort of up in the air.

William Binney, A72, gave a very elementary example of the application of Set Theory in a context where most analysts would consider it an intuitive thing. The example assumed complete knowledge of a callsign system so that a given call could be identified as coming from a given book. The example showed several "Military Regions" and their book usage.

	SET A	B	C
Region I	(Book) 1	2	3
Region II	3	4	5
Region III	5	6	7
Region IV	7	8	9
Region V	9	10	1

(Sets represent certain date periods)

Intuitively, we say that a callsign from Book 2 is (was) used only by MR I, while Book 5 is either MR II or III. This can be presented in a Venn diagram:

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

Again, very basic, but an application not usually considered in the realm of math by the layman.

Dr. Reed Dawson, P12. Dr. Dawson's lecture on Set Theory and Probabilities was addressed to the problem of trying to determine how much of the total traffic transmitted we actually intercept. Sorry I can't go into more detail because the math was not intuitively obvious to the casual observer.

The last speaker was Gary again. This time he gave illustrations of actual Soviet problems of the early 1950s. The one I'm most familiar with (the technique, that is) is the diagnosis and

Gary concluded with the observation that we have been doing analysis for a long time. He wondered if we were dealing with new concepts (math applied to analysis) or just new names of techniques.

I guess the real impression I got from the symposium was one of re-emphasis on the idea that not many of the cryptologic disciplines are pure. We are always applying whatever talents we have to the job at hand and don't worry too much about names or titles some people apply to the things we do. But it is refreshing to find again that many of the disciplines are not steeped in "Black Magic," but are based on common sense and basic knowledge of how things work. I think, the next time one of my analysts complains about routine, so-called "flunky" work, I'll try to impress upon that analyst all the different, ostensibly esoteric, techniques that are applied on a routine basis."

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3(h)(3)  
PL 86-36/50 USC 3605**SEEDLINGS**

----Grids for the new positions of the B forward outpost relocated to FANX II from FANX III on 20 November 1972 are: A2540--B1, A2E72--B11, and A2548--B12. Operating frequencies are unchanged.

\*\*\*\*

----Employee recognition: "All of you who are supervisors, especially, take care of your people. Recognize their work. Let's do all that we can to reward their performance." This quotation from Lt Gen Phillips's opening remarks on assuming the Directorship should be noted by all supervisors regardless of their position in the chain of command.

The Agency's Incentive Awards Program provides one means of recognizing employee accomplishment. For many personnel, "Employee Suggestions" are synonymous with the entire awards program; most frequently they are unfamiliar with its many other aspects.

Visible evidence of the variety of employee awards--cash and honorary--sponsored by NSA was recently on display in the passageway between Gatehouse One and the Operations Building, and in the case on the south side of the Operations Building, 1st floor escalator. All personnel,

especially supervisors, are encouraged to become familiar with the numerous awards which are available to recognize employee accomplishment.

The NSA Personnel Management Manual, Chapters 503 and 504, identifies these awards, outlines eligibility criteria, and advises on procedures for initiating and submitting recommendations. Information and assistance are also available from the Incentive Awards Branch (M362), Room 1A190.

\*\*\*\*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

----Speeders beware! MPs at Ft Meade are using a "Buck Rogers" contraption to measure auto speed. It is hand-held, can operate from a patrol car battery or portable battery pack, and is accurate to one-tenth of a mile per hour. The radar gun sends a radio signal to the observed car. The signal bounces back and the speed is indicated to the MP operator.

\*\*\*\*

----The NSA International Affairs Institute is trying to obtain George F. Kennan of Princeton to open the 1973 lecture series. Other speakers being sought for 1973 are Charles Bohlen, Arthur Schlesinger, William Buckley, one of the Rostow brothers, Zbigniew Brzezinski of Columbia, K. Galbraith, and Admiral Kidd (ex-Commander of 6th Fleet). The final lecturer of the 1972 series will be a U.S. diplomat speaking on Latin America (probably Chile).

The Institute has started to explore the feasibility of implementing its other objectives, i.e., SIGINT report writing and SIGINT seminars. Since the matter is somewhat complicated, could we ask the readership of *Dragon Seeds* for ideas on these two goals? Incidentally, IAI member Dick Seron of B6 has already presented his views on seminars; possibly other readers have something to contribute.

Our membership drive for 1973 will begin the first week in December. Since the type of lecturers depends largely on what we can offer as honorarium, we are seeking increased participation. Dues of \$3 per year may be forwarded by check to Mr. James Duncan, Pl. Be sure to include your name, organization, and both telephone extensions.

\*\*\*\*

---B Group cryptanalysts should be wary of the STET program included in the IBM 370 RAPIDS package. During her recent tour in B1203, Dr. Marti Branstad identified serious errors in the polygraphic repeats portion.

\*\*\*\*

Behold the turtle! He makes progress only when he sticks out his neck.

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

ASK  
THE  
DRAGON  
LADY

Dear Dragon Lady:

What are the views of the TACP on changing jobs to benefit from points awarded for experience?

--An Aspirant

Dear Dragon Lady:

Why does the TACP not accept applications for the TA Intern Program if they have had more than two years cryptologic experience? The selection criteria referring to experience states, "...must ordinarily have at least one year of TA experience at minimum GGD-07 or E-5 level; however, must not have more than two years of cryptologic experience at GGD-07/09 levels." (See OM, Subject: NSA Intern Program Vacancies, dated 28 August 1972.)

--Piqued

*The Dragon Lady asked the Executive of the TA Career Panel to comment on the above questions. His views follow:*

Dear Aspirant:

The TACP has recognized that there are benefits to be derived from exposure to different types of targets, and has specifically organized its PQRS to encourage movement of TA aspirants between different TA problem areas. Bonus points are awarded in one lump sum of 140 points for a second exposure; this implies that the first exposure consisted of

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

at least one year at the GGD-07 level or military equivalent or at the GGD-05/E-4 levels where it can be shown that this experience equates to the higher grades. Point values for TA experience are allocated at the rate of 15 points per month for the first two years of creditable experience, 10 points per month for the third year, 5 points per month for the fourth year, and 2 points per month for the fifth, sixth, and seventh years. The declining point allocation is intended to prompt rotation to gain diversification on another problem, e.g., if an individual remains on the same problem (same category of creditable TA experience) for seven full years under the present criteria, he can accrue only 612 points of a possible 750 maximum. One year in another creditable experience category would gain him the 140 bonus points or maximum in experience. A revision to the criteria is currently being typed which allows more points for the fifth, sixth, and seventh years of TA experience and broadens the exposure areas for bonus awards. Watch for the revision, which will be on the streets hopefully before the first of the year.

\*\*\*\*

Dear Dragon Lady:

I am writing to express my feelings about the various informal prep sessions held prior to the CA PQE. As you are probably aware, these sessions are given by A, B, and G to acquaint their personnel with the types of questions contained in the exam. When one considers the logistics involved in staging three separate sessions, the mind boggles. For example, regardless of the length of the class (less than 30 hours for B, and more than 200 hours for A), you still have three classroom facilities, three sets of study materials, and three sets of instructors.

Enter my theory: I would like to suggest a single prep class, sponsored by the CA Career Panel. This class would be open to all persons eligible to take the PQE regardless of group affiliation. One of the benefits of this would be the elimination of two classroom facilities, two sets of study

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

materials, and two separate sets of instructors. Another benefit is that the CA Panel has access to the best qualified instructors for any given phase of problems, and knows the material which will be contained in the exam. Then, personnel in B or G, who currently spend less than 50 hours on preparation, will not be any less prepared than personnel from A, who currently spend more than 200 hours in preparation.

Respectfully,

MORRIS L. FERGUSON

Dear Morris:

Mrs. Wilma Davis, CACP Executive, tells us that the Panel views provision of training for non-interns as a proper function of line management. The Panel evaluates PQRs submitted by individuals and recommends specific training courses that would be of value in pursuit of professionalization. To that extent, it provides individual help in preparation for the PQE. The CACP does not involve itself in actual teaching, but has provided teaching materials and suggested study aids to organizations and individuals as special help in preparing for the exam.

We asked the same question of three other career panels which include a PQE in their certification procedure. The Traffic Analysis Panel looks with favor on the offices' providing such training and has supplied material for their use. Like its crypt counterpart, the TA Panel does not itself engage in teaching. The Special Research Panel considered our query a bit premature, since the PQE for that field is still being evaluated. The SR Panel does intend to provide to individuals preparing to take the PQE a study guide which will be available to them about two months before the date of the exam. The main concern of the Data Systems Panel is at present its interns, but it is considering the possibility of providing special help to non-interns getting ready for the PQE.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

To Virginia and Meech, who asked, "How do you get a job on a career panel or in its executive office?"

Again, our source of information is Mrs. Wilma Davis, CACP Executive, who tells us that Panel members and the Panel Executive are appointed by ADPM upon recommendation of the Panel Chairman. The two technical assistants to the Executive are appointed by the Panel and serve for two years. They, like the administrative and clerical assistants, are attached for administrative purposes to the organization to which the current Chairman of the Panel is assigned. A vacant assistant job may be filled by advertising or by inter-organizational transfer. If you are interested, you may want to talk to the panel Executive.

\*\*\*\*



*"Please let me see my article in Dragon Seeds..."*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~SOLUTION:

G L I M P S E S O F T H E S A G E S O F C H I N A  
 9 15 13 16 20 21 4 22 18 7 25 11 5 23 1 10 6 24 19 8 3 12 14 17 2  
 C O N F U S I U S M A I N T A I N E D T H A T G O  
 O D G O V E R N M E N T O B T A I N E D W H E N T  
 H E R L E R W A S R U L E R A N D T H E M I N I  
 S T E R M I N I S T E R X W H E N T H E F A T H E  
 R W A S F A T H E R A N D T H E S O N S O N X T H  
 A T S O C I E T Y W A S A N O R D I N A N C  
 E O F H E A V E N A N D W A S M A D E U P  
 O F F I V E R E L A T I O N S H I P S X X  
 R U L E R A N D S U B J E C T H U S B A N D A  
 N D W I F E F A T H E R A N D S O N E L D E R B R  
 O T H E R S A N D Y O U N G E R A N D F R I E N D  
 S X X R U L E S S H O U L D B E I N R I G H T E O U  
 S N E S S A N D B E N E V O L E N C E O N T H E P  
 A R T O F T H E F I R S T F O U R X S U B M I S S  
 I O N T O R U L E S S H O U L D B E M A R K E D B Y  
 R I G H T E O U S N E S S A N D S I N C E R I T Y  
 X X B E T W E E N F R I E N D S X T H E M U T U A  
 L P R O M O T I O N O F V I R T U E S H O U L D B  
 E T H E G U I D I N G P R I N C I P L E X X O F A  
 H E R E A F T E R X H E D I D N O T T E A C H X X

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

$Z_1$  and  $Z_0$  are non-textuals: the first contains the number of unused cells in the matrix and indicates the key column under which the diagonal (comprised of the first four groups of cipher) was extracted. The second non-textual contains the group count of the message.

\*\*\*\*

Answers:

1. Repeating key
2. Playfair
3. Stubby
4. Coincidence
5. Periodic

Cryptoanswer:

Fibonacci

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3(h) (3)  
PL 86-36/50 USC 3605

## CONTRIBUTORS

WALTER D. (JOE) ABBOTT, JR., B605, received his B.A. in English literature from Harvard College in 1960 and entered the Army Security Agency shortly thereafter. Among his Army experiences were a year in Monterey studying Chinese-Mandarin and a two-year tour in the Philippines as the OIC in the Processing and Reporting shop for the now defunct USM-9. He joined NSA in 1966 and had a tour in Hawaii, during which time he was the NSA Pacific representative to the CINCPAC IGC working group. A certified Special Research Analyst, he is currently the Chief of the Intelligence Staff for all Communist Ground Force activity in Southeast Asia.

JEAN F. GILLIGAN, B32, was graduated from Duquesne University, Pittsburgh, Pennsylvania and pursued graduate studies at Catholic University, Washington, D.C. She entered on duty with NSA in December 1968 with the PRC [redacted] Division Intelligence Staff. Mrs. Gilligan is presently assigned as the acting chief of the [redacted] Section of the PRC [redacted] Branch. She is responsible for the entire production of the PRC [redacted] as well as research and reporting of PRC [redacted] activity.

TOM GLENN, Chief, B61, has a total of 14 years experience with ASA and NSA on the Vietnamese problem. He is a professional Special Research Analyst and Vietnamese linguist who has also studied Chinese and French on his own. Mr. Glenn has served as the Chairman of the Vietnamese Language Professionalization Examination Committee. Assigned to Vietnam in 1962-65, 1967-68, and 1969, he has been involved in traffic analysis, cryptolinguistics, intelligence analysis, and most significantly, in the management of the SIGINT reporting effort on the Vietnam war.

LOU GRANT is a professionalized Special Research Analyst with over 22 years Agency experience. He spent the first 15 years on B Group problems, working as a traffic analyst, reporter, and staff officer. Since leaving B Group, he has served as an Assistant Inspector General, Administrative Chief for NSA Europe, and is now an Action Officer in ADPSD.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3(h) (3) PL 86-36/50 USC 3605
---------------------------------------

PHILIP REMSBERG, B41 Machine Applications Project Team, majored in industrial psychology at Gettysburg College and Penn State University. He entered on duty with NSA in 1966 after having completed a three-year tour with the Army Security Agency. Within B41, Mr. Remsberg has worked as a traffic analyst, callsign analyst, and practice systems analyst, with special attention to machine applications against his target problems. He is now engaged in information design studies specifically concerned with the impact of AG-22 on B41 operations.

E. LEIGH SAWYER, Chief of B02, majored in Romance languages as an undergraduate at Harvard, and attended the Chinese Language School (Hua Wen Hsueh Hsiao) at the University of California Berkeley while in military service. He subsequently served with a Chinese Army Command in Nanning until VJ Day, and left China in 1947 following G2 and Assistant Military Attache assignments in K'unming, Shanghai, and Nanching.

JACK SHARRETT, B603, joined the Agency in 1962 after receiving his Bachelor of Music degree from the University of West Virginia and completing a six-month tour in the Army Reserve in which he served as a Munitions Transshipment and Storage Specialist. Hired by the Agency as a cryptanalyst on the Soviet [redacted] problem, he shifted within six months to B Group and a Vietnamese translation course. His ten-year tour as linguist, cryptanalyst, and reporter in various B6 elements has been highlighted by assignments to the NVN Navy problem, Civil and Diplomatic problem, and a TDY to Phu Bai on VC Tactical Military and General Directorate of Rear Services problems. In B603, he is primarily concerned with the training and assignment of linguists in B6 and the maintenance of RICE BOWL, the computerized Viet-English dictionary.

DAVID J. TIREN, B61, plied the trade of ASA intercept operator for six years. He accepted a position in the original NSA Civ Op program, serving in Kyoto, Japan, for two years in the late fifties. Later, after six years as a Traffic Analyst in A6, he spent 1964 as a member of Class Five, CV-100. Assigned to B6 in early 1965, Mr. Tiren has had a variety of exposures and emphases. He is currently Chief, B612, a branch whose responsibilities in the North Vietnamese non-Morse communications area include tank-to-tank communications (see September DRAGON SEEDS).

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

*NORMAN WILD, B03, is one of the Agency's foremost multilinguists. He has been with NSA and predecessor agencies since September 1944, working mainly with Far Eastern languages. (It is reliably reported that he reads STC like plain language.) Mr. Wild's academic background includes the B.A. (1939) and the M.A. in Chinese and Japanese (1941) from Columbia University. He is the author of numerous linguistic reference and training aids within NSA, and has long been concerned with the interplay of computers and language.*

**TOP SECRET UMBRA**

*it's*

*classified!!!*

~~TOP SECRET~~

# National Security Agency

Fort George G. Meade, Maryland



MARCH 1973



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~TOP SECRET UMBRA~~

This is *Dragon Seeds*.

There is fantasy, irony, and the bite of reality in the name. It speaks of the East. And, like the East, it suggests much, says little.

*Dragon Seeds* is both Mother China and her neighbors. *Dragon Seeds* is monumental and minuscule. It is the past and future. It begs for elaboration but gives none. In it are echoed softly slurred Mandarin, brittle Vietnamese, determined Korean. In it is the spectre looming over the Thai, Lao, and Khmer. It is frightening and friendly. It is uncertain.

Above all, *Dragon Seeds* is promise. It is fertile with ideas unbounded, to be cultivated with creativity and imagination. It is challenge. It is alive. It will be more than it is.

*Dragon Seeds* is yours. May it grow with you.

The Editors

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

PL 86-36/50 USC 3605

DRAGON SEEDS

Publisher

DONALD E. MC COWN, CHIEF B03

Managing Editor

Minnie M. Kenny

Feature Editor

Richard V. Curtin

Rewrite Editor

Victor Tanner

Executive Editor

Robert S. Benjamin

Biographical Editor

Jane Dunn

Education Editor

Marian L. Reed

Special Interest Editor

Ray F. Lynch

Composition  
Composition

Helen Ferrone  
Lorna Selby

PRESS CORPS

B11 Carolyn Y. Brown

B12 Philip J. Gallagher

B2 Dee Ensey

B31 Jack Spencer

B32 Jean Gilligan

B33 Louis Ambrosia

B34 Thomas L. Wood

B41 James W. Schmidt

B42 Peggy Barnhill

B43 Mary Ann Lasle

B44 Jack L. Thomas

B45 John E. Uzarek

B5 Nancy Fournier

B61

B62 Edmond J. Guest

B63 George S. Patterson

B63 William Eley

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



VOL 2  
NR 1

MARCH 1973

**TABLE OF CONTENTS**

The Jack Butcher Case. . . . . William G. Flynn 1

Rebels in Thailand . . . . . Geoffrey Wood 6

A Gist of the Korean SIGINT Problem. . . . Richard S. Chun 12

SIGINT Support on the Economic Front . . . . William Hunt 18

The Ground Zero Approach to Language  
Analysis. . . . . Dan Buckley 22

Exploiting the Bust. . . . . Kenneth Miller 25

Once More the TSR. . . . . Jane Dunn 29

How About the Oldsmobile M?. . . . . Thomas Wood 32

Standardization???? . . . . . Russ Myers 33

Seedlings 34

Ask the Dragon Lady 38

Contributors 45

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

# NG ÆNG BẮN



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

THE JACK BUTCHER CASE

by William G. Flynn, B6

On 24 March 1971, North Vietnamese ground forces shot down a USAF OV-10 twin engine reconnaissance aircraft in the Saravane area of Laos. The aircraft was piloted by 1st Lt Jack M. Butcher, who was believed to have been injured in the crash. He was, however, able to make a voice transmission prior to his capture by enemy troops. Communist communications of 25 March reported that an AAA battalion of Binh Tram 34 had shot down an OV-10 aircraft, and that they had captured the pilot alive. Normally this would have been the end of it, for SIGINT reflections of pilot captures were noted frequently over the years. But this time it was not the end. It was just the beginning of a saga in which SIGINT played a very important role.

One month later, on 26 April, a message was intercepted which pertained to Lt Butcher, discussing the capture of an American and describing him as an "intelligence type" (a term used for OV-10 pilots, indicating visual reconnaissance). Butcher had apparently received injuries during the crash. This was indicated when a Rear Services element reported that the American POW had "fully recovered" and preparations were being made to transport him north through the Rear Services system. His captors were instructed to send him "up" quickly so that he could be interrogated. Apparently he had not been questioned since his capture because no one in that area spoke English.

On 7 May, a commo-liaison station of Binh Tram 14 was instructed to prepare to receive the "pirate POW" who was being escorted by two infantry cadre of Binh Tram 34. The stations were cautioned to be extremely vigilant in handling the prisoner because he was a "die-hard"--apparently meaning that they were having difficulty handling him.

Sometime during the next two days, while being transported north, Lt Butcher escaped, thus starting a series of events that was unprecedented in the history of SIGINT support to Search and Rescue (SAR) efforts. The message that triggered a massive recovery effort was intercepted on 9 May and revealed that "a lieutenant, an OV-10 pilot, being brought to the rear had escaped due to our negligence." The message described the

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

lieutenant as "a spy" and "very dangerous" and further stipulated that if he was not captured, "he may cause damage to our entire system." When this message was received by the SIGINT Support Group for the Special Operations Group of MACV, the Joint Personnel Recovery Center (JPRC) was notified immediately. The JPRC commenced a check of OV-10 pilots known to have been downed in that area and confirmed that the prisoner referred to in the message had to be Lt Butcher. Lt Butcher's escape, evasion and recovery plan was then reviewed and a determination was made as to his probable direction of travel in his attempt to be rescued.

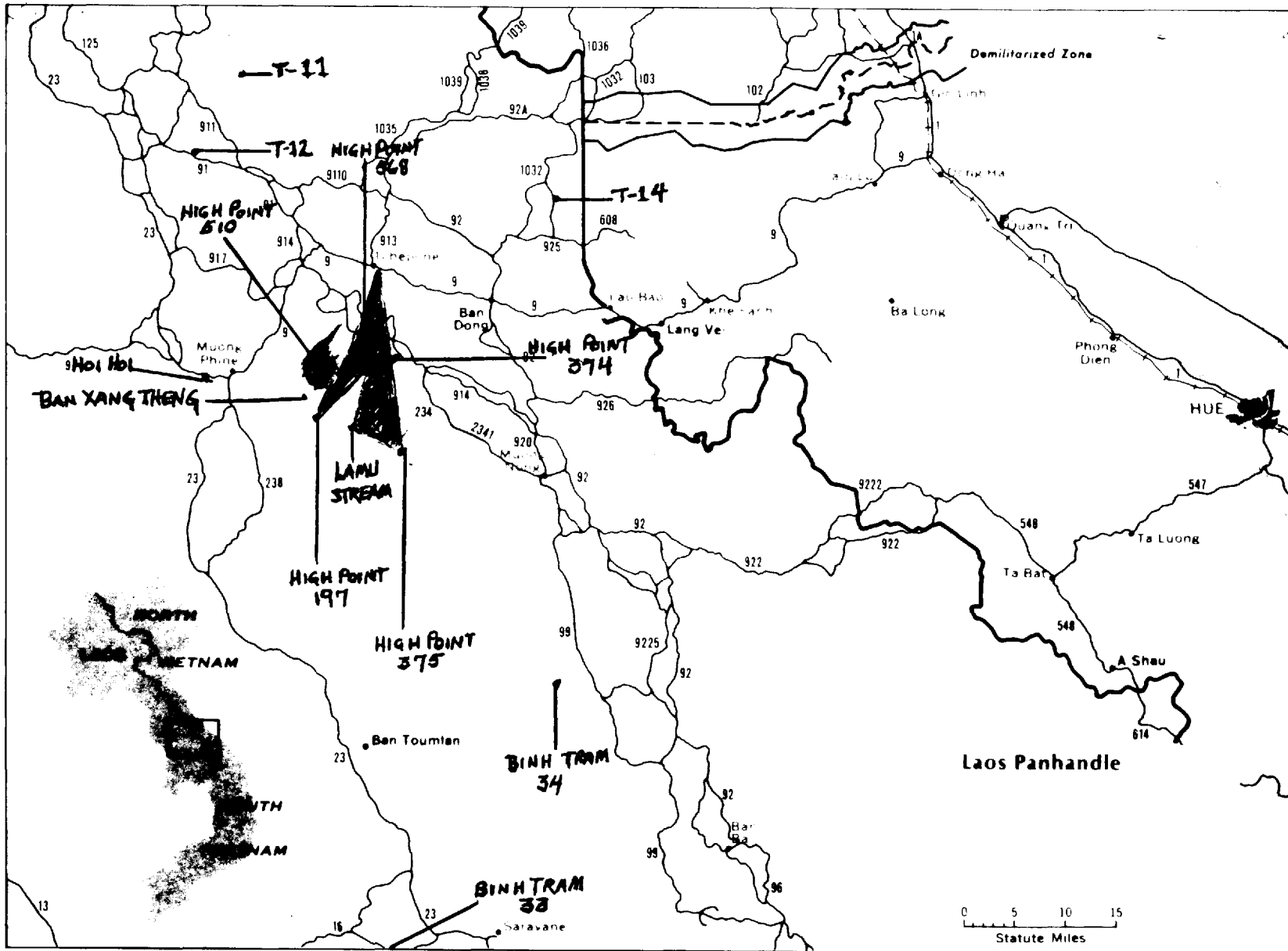
The following day, another intercepted message gave a description of the escaped POW and notified all units to be on the alert. Lt Butcher was described by the Hq 559th Transportation Group as still in uniform and wearing boots. Shoes were generally the first thing to be taken from a prisoner. This then indicated that he had been giving his captors trouble and had not accepted the fact that he was a prisoner of any permanency.

It was at this point that NSA became actively involved for the first time in a real-time recovery of a downed pilot. In addition to the normal reporting conducted by field elements, messages and technical back-up material concerning the plight of the American pilot were being forwarded to NSA via OPSCOMM immediately after intercept. This material was then reviewed and retranslated in an attempt to derive any possible additional information. I want to stress at this time that this action was not taken because we thought that the field stations were not doing an outstanding job--they were--but to emphasize the importance placed on the recovery of this pilot. For the next 20 days NSA had both linguists and technicians available on a 24-hour basis to assist in the recovery attempt.

The Communist search intensified. Binh Tram 33 instructed units to "motivate the specialized forces at the district" and to send someone down to the hamlets of Du Mong, Bang Xang Theng, and Hoi Hoi to discuss the matter with local force cadre and the troops of the Peoples Army at Tchepone. They were directed to "search until they find him." The fate of Lt Butcher was very much on the minds of the U.S. military commanders in South Vietnam. Captain Bill Coenen, USMC, chief of the SIGINT Support Group, was called upon to give a briefing on the Lt Butcher escape and recovery actions to General Abrams, CONUSMACV.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

General Abrams ordered that all available assets be placed at the disposal of the Joint Personnel Recovery Center. The 7th Air Force made all its resources available, and moved helicopters to areas adjacent to the area in which it was believed that Lt Butcher would attempt to reach for recovery. In addition, daily photo missions were flown over this area for any sign of his whereabouts.

Communist entities in the Binh Tram 33 area continued to search for the escaped OV-10 pilot. On 13 May, it was reported that the Communists had formed two small teams which were searching in the area of High Point 568, High Point 197, and back to Tchepone. Upon arrival at Tchepone, they were instructed to search in small circles around the Lamu Stream and back to High Point 375 and eventually to an unspecified new storage area. Additional teams were ordered to investigate caves and streams in the vicinity of High Point 510 with great care. At this point, the Communists appeared to be sure that the pilot was still in the area of a new storage facility and concentrated their search in that area.

The search for Lt Butcher was one week old when, on 16 May, Communist units reported that on the previous day Allied helicopters had searched "area two" all day. Later the same day, another message disclosed that the "screeching owl," a derogatory term they were using to refer to Lt Butcher, was in "area one" and ordered that a sweep be carried out through that area. The search was to focus on "streams, rocky fields and cultivated fields," with particular attention on "high trees." One main search element was dispatched to the location where the "escaped enemy" was first seen.

There was no celebration of Ho Chi Minh's birthday for Communist forces in the Binh Tram 33 area because, as of 19 May, Lt Butcher was still at large and the search continued.

Lt Butcher had evaded his captors for about 10 days now, and yet, with all the Allied assets dedicated to his recovery, we still had been unable to rescue him. The time had now come to take a calculated risk. Aircraft equipped with loudspeakers were flown over the area we knew the Communist forces were searching. They attempted to contact Lt Butcher by broadcasting to him, using prearranged information contained in his escape, evasion and recovery plan, in an attempt to establish a rendezvous point for his extraction. The question at this

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

point was, would this compromise our SIGINT effort, or would the Communists merely surmise that Lt Butcher had been able to contact Allied forces. Whatever the thoughts of the Communists were, we will probably never know. But one fact is sure, we did not lose our intelligence collection from these units.

The broadcasting did not go unnoticed by the Communists, because on 20 May the Combat Operations Section of Binh Tram 33 reported that an OV-10 had used a loudspeaker to contact the pilot by secret means in areas one and two. As a result of this action, Communist forces sent out three search teams to form an ambush; but their efforts were in vain, since a later message revealed that the OV-10 pilot was still loose in the area. Another insight into the dilemma of the Communist forces searching for Lt Butcher was their concern, expressed by Binh Tram 33, over the possibility that civilians were assisting the pilot. It was suggested that a "proselyting team" be sent into the area to determine if civilians were hiding the POW.

Lt Butcher was probably recaptured by the Communists on 26 May after about seventeen days of evasion and living off the countryside. On 27 May, a dispatch from the Military Movement Section contained information concerning the northward movement of an American POW who was very stubborn, had escaped once, and had to be tied up. The report listed the prisoner's height as 1.8 meters and reported his name to be "BOOTS SOW," an apparent transliteration for Butcher. It was also reported that the American was white, had three broken teeth, and was wearing a black shirt, underwear, and long military trousers. Of interest is that in this instance no mention was made of his "high boots." Apparently the Communists had learned their lesson.

A few weeks ago, when the names of 10 POWs held in Laos were handed over to Allied authorities, Lt Jack M. Butcher's name was on that list. For a great many of us, this news had deep personal meaning. Hopefully, another chapter in the Jack Butcher case can be written at a later date, giving his side of the story.

~~TOP SECRET UMBRA~~


~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

REBELS IN THAILAND

by Geoffrey Wood, B12

Since taking up arms against the established government in 1965, Thai insurgents have slowly and steadily grown in number and effectiveness, their activity marked by ever expanding use of modern weapons and skillful guerrilla tactics with one puzzling exception



Communism in Thailand

At least as early as 1920, the Bangkok Chinese community was sending funds to support Communist activities in both China and India, and agents from those countries were busily soliciting funds and talking of future revolution in Asia as an inevitable consequence of the Soviet revolution. Small cells were established, chiefly among students and members of the Chinese community in Bangkok. In the late 1920s, Nguyen Ai Quoc (Ho Chi Minh), disguised as a Buddhist monk, spent several months in Thailand propagandizing the Vietnamese colony and establishing a Communist youth organization. Later, many of these youths became leaders in the Hanoi regime. Activity among the Thai themselves was minimal, and Communism was generally regarded by Thai officials as a foreign import without much appeal to the generally contented and racially homogeneous Thai. In an effort to divest the movement of its foreign--particularly Chinese--flavor, the Communist Party of Thailand (CPT) was founded in 1942, but its failure to dominate the World War II Free Thai anti-Japanese movement, as well as its inability to generate an active insurgency at the war's end (the only South-east Asian Communist party that failed to do so), attest to the Party's weakness and its lack of appeal to the Thai.

Foreign influence and support continued, with Communist China training exiles who provided leadership in the CPT. During the late 1950s and early 1960s, North Vietnamese agents active among Vietnamese refugees in Thailand helped to set up the insurgency which was soon to follow. Arrangements were probably made at this time for training of Thai Communist recruits in North Vietnam and in Communist-controlled areas of Laos.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Open rebellion began in 1965, before adequate foundations were fully laid. This premature action was probably taken at the urging of the Chinese and North Vietnamese to divert U.S. attention and resources from Vietnam and Laos, and perhaps to discourage the Thai government from more active participation in the Indochina war. The insurgents' decision to take up arms was announced from China by both Radio Peking and the Voice of the People of Thailand (located near Kunming, in Yunnan Province). Peking's announcement of Communist plans for Thailand suggests that China had a significant role in formulating the decision.

#### Insurgency Now

With fewer than 6,500 effectives in a population of 35 million and only about 1,000 CPT members, the insurgent movement does not now pose a threat to the regime. The government continues, however, to be troubled by its activities in remote areas where central authority is weak or non-existent.

The insurgency differs significantly from one region of the country to another. In the far South, where some 1,400 men are under arms, the insurgency is unusual; it is neither under the direction of the CPT nor directed against Thailand. The insurgents there are mainly ethnic Chinese, veterans of the Malayan insurgency of the 1950s and younger recruits. Their allegiance is to the Communist Party of Malaysia, and they are targeted primarily against Malaysia. Although they are not really a part of the Thai insurgent movement, they do pose a threat to governmental authority in the area.

In contrast to most of the country, the Northeast, the site of the first active insurgency, is plagued by drought and a chronically depressed economy. There are ethnic differences between the northeasterner and the central Thai; the region borders on the Laotian Panhandle and the northeasterner is culturally and linguistically more Lao than central Thai. The Communists play upon the cultural differences and on the desire of the villagers for a share in the apparent affluence of the central plain. In addition to sheltering about 2,200 insurgents, the Northeast is also the location of approximately 40,000 Vietnamese refugees who are ideologically loyal to Hanoi. They have not been closely involved in the insurgency, but the Thai view cooperation between the refugees and the insurgents as an ever present danger.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The insurgents in the Northeast are capable of low-level attacks on small Thai government units and installations. Poorly armed initially and without an adequate local support base, the insurgents were repulsed in early confrontations with the government. Since 1967, they have utilized more cautious tactics, avoiding direct confrontations with counter-insurgency forces, while improving the quality of their organization and the security of their village support bases. Recently, they have emphasized political indoctrination, establishment of village military units, and acquisition of more sophisticated small arms. They probably have influence over a population base of at least 100,000 people in the Northeast.

Insurgency in the North, which broke out actively in 1967, was marked from the beginning by the participation of hill tribesmen, principally Meo, reportedly lead by Sino-Thai cadres. There has long been ill will between the ethnic Thai who live in the lowlands and the Meo tribesmen who resent efforts by the government to curtail their slash-and-burn agriculture, which damages the valuable teak forests. Recent attempts by the government to end the cultivation of opium have led to further friction, sale of opium being the sole source of cash for most of the hill people. Government losses in the North have always been heavier than in the Northeast, principally because the Meo had modern small arms and were fighting on their own rugged mountainous terrain. The Thai reacted to losses on occasion by indiscriminate bombing of mountain villages, which caused great resentment without inflicting any damage on the insurgents.

Because the insurgents were Meo and not Thai, the central government was not overly concerned by events in the North. Even the establishment of secure base areas in some of the rugged mountains bordering Laos did not appear to worry Bangkok. With evidence of Communist success in recruiting ethnic Thai villagers over the past two years, the government began to take a more serious view of the situation. Security forces mounted a so far unsuccessful effort to establish a presence in the mountains along the Laotian border.

The northern insurgents, avoiding major contacts except when the odds were in their favor, carried out intensive harassment of government operational bases in isolated areas and conducted effective ambushes along principal lines of communication. Their tactics included coordinated attacks by groups of

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

up to one hundred men and well executed ambushes by large groups employing mines and booby traps. They routinely used automatic weapons (AK-47) against both personnel and helicopters, and often used rocket launchers (M-79) in harassing ground elements. Their arsenal included anti-personnel mines, especially a plastic Soviet type, and in March 1971, they employed rocket-propelled grenades to destroy an armored personnel carrier (APC), the first confirmed insurgent use of this weapon. At the end of March, an APC detonated an anti-tank mine, again the first use of such a weapon in Thailand. The insurgents operated effectively in platoon and company sized units.

#### Insurgent Communications

The skillful use of sophisticated weapons clearly reflects the support given by the Chinese Communists and the North Vietnamese.

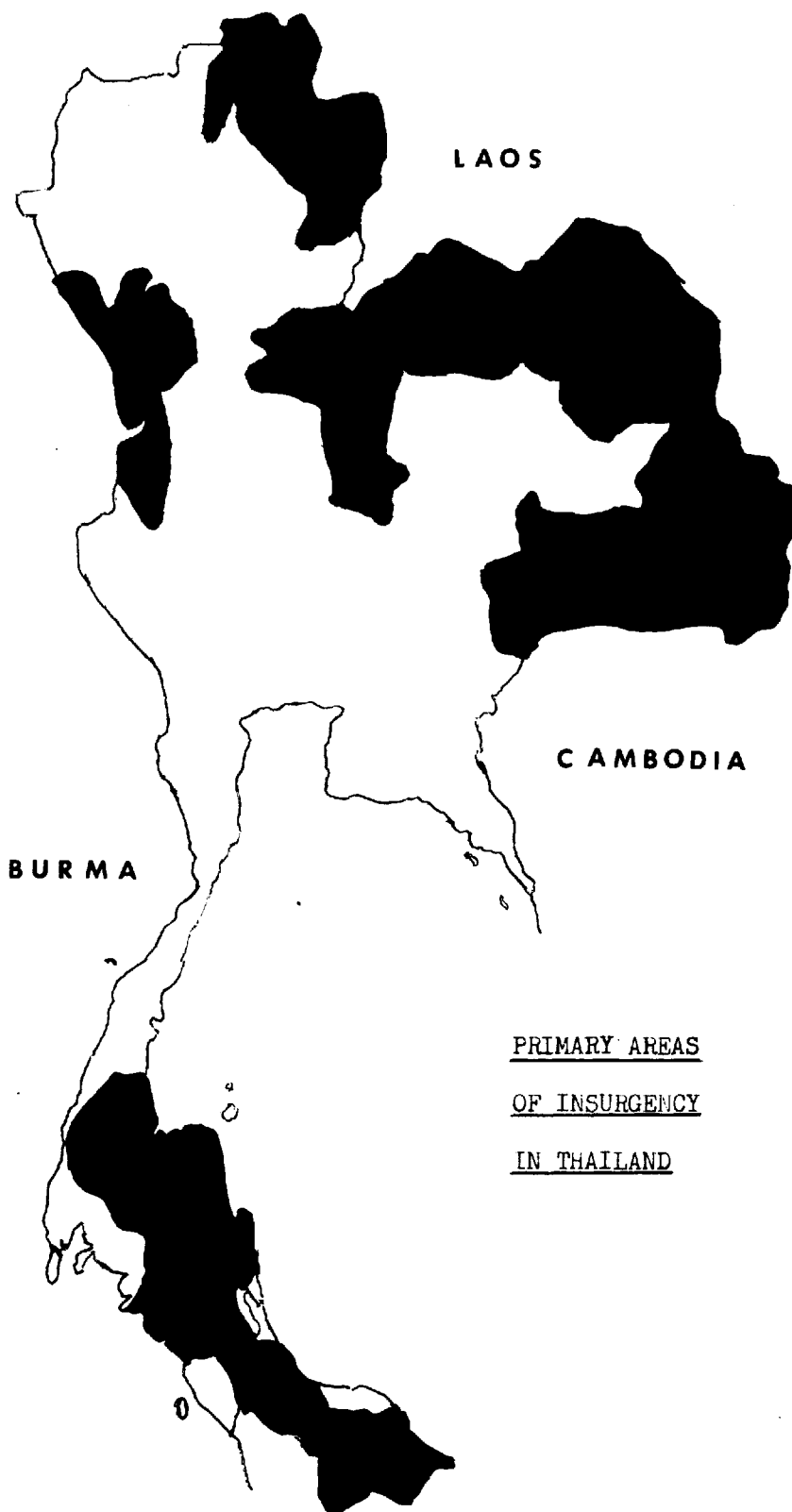
There are numerous reported sightings of insurgent groups carrying radios. Interrogations and inspection of captured radios show most of these radios to be transistor receivers used for listening to Communist propaganda broadcasts. No captured rebel has ever admitted to insurgent use of radio communications, although detailed descriptions have been obtained of courier communications. A collateral report has furnished a wealth of information on training given in North Vietnam and Communist China to six insurgents. They trained for four years in the use of radios for communicating. Nevertheless, the trainee who defected had not seen or used a transmitter in the two years between her return to Thailand and her defection in 1968. Other collateral and interrogation reports document radio facilities serving Pathet Lao support bases along the northern Thai border with Laos. Messages are reportedly passed by courier to these facilities for relay to external addressees.

#### Radio Search Efforts

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



There is conclusive evidence that both the Communist Chinese and the North Vietnamese (to include their Laotian clients, the Pathet Lao) actively support the insurgency in Thailand. The support encompasses training at all levels, material supply, the provision of safe havens, and high-level policy guidance. Communications of these countries may well be involved in support of the Thai insurgency, perhaps intelligence, security, party, military, and press.



The insurgency, though small, is growing, and insurgents have become increasingly sophisticated in their tactics and employment of weapons, particularly in North Thailand.



~~TOP SECRET UMBRA~~

EO 3.3b(3)  
EO 3.3b(6)  
PL 86-36/50 USC 3605

A GIST OF THE KOREAN SIGINT PROBLEM

by Richard S. Chun, B44

Prior to June 25, 1950, when North Korean forces crossed the 38th parallel, there was virtually no SIGINT effort on North Korean communications. A U.S. Army Security Agency unit (ASA Pacific) in Tokyo, Japan began intercepting North Korean traffic. This effort was later augmented by a South Korean intercept source (ROKN Group "M"). ASA Pacific established an advanced element in Taegu, Korea in September, 1950; and by mid-October, the 60th Signal Service Company (330th ASA Company) from Fort Lewis, Washington, arrived in Pusan. Total intercept was thus increased to 20 positions.

The increased collection of North Korean communications introduced a need for traffic analysts, cryptanalysts, and linguists. There were no Korean linguists assigned to the Armed Forces Security Agency (NSA). One male civilian who had studied the language while hospitalized and a female civilian of Korean descent, both employed by NSA, [redacted] established the first Korean language unit. [redacted]

The unit was augmented when reserve officers with previous Korean language background were recalled to active duty; and the Army Language School (DLI/W) at Monterey, California assisted by accelerating its training of U.S. military personnel in the Korean language. Meanwhile, two U.S. Army officers of Korean ancestry, stationed as instructors at the Army Language School, were assigned to the Army Security Agency and transferred to ASA Pacific, Tokyo. They were later joined by several NSA linguists. (One of the instructors was LTC Youn P. Kim-- probably the greatest single contributor to the North and South Korean SIGINT effort.) Complicating the shortage of Korean linguists was the almost total lack of suitable Korean dictionaries and knowledge of North Korean military and technical terminology. A file of terminology appearing in North Korean military communications was compiled. Definitions of terms were determined by context and by reference to Japanese and Chinese dictionaries. The file was supplemented by data from prisoner of war interrogations, conducted by the two ASA officers, and by captured North Korean documents obtained through various U.S. military sources.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

Much cryptanalytic success was achieved early in the war, and NSA and field personnel gleaned highly perishable intelligence information from decrypted messages. Most North Korean messages at this stage of the war were enciphered with low grade cryptosystems which changed frequently but remained unsophisticated in complexity. Voluminous end product translations produced during late 1950 and early 1951 were of great value to intelligence users. Messages emanating from high echelon North Korean sources revealed significant information concerning the capabilities and intentions of North Korean forces. Users for the United Nations forces considered this a valuable source of information. It has been estimated that approximately 85% of the total usable intelligence information during this period was furnished by cryptologic sources.

Exploitation of North Korean cryptosystems and translation of messages was hampered more by the sheer volume of messages than by the complexity of the systems themselves. Large volumes of significant message decryptations had to be published by a small work force. However, by the Spring of 1951, the cryptosystems became more sophisticated and exploitation became increasingly difficult. This was often attributed to the intervention of Soviet advisors who apparently became alarmed over the lack of communications security. Despite increased security efforts, U.S. cryptanalysts were successful until the fall of 1951, when North Korea first introduced "pad" encipherment. The percentage of exploitable messages dropped, less plaintext was used, and the overall intelligence furnished by SIGINT decreased.

Traffic analysis posed no problem during the hostilities. Most of the callsigns, frequencies, identifications, and locations of North Korean forces were recovered from decrypted messages. Following the truce, however, traffic analysis was a painstaking problem. Progress was finally made when North Korea began using [REDACTED]

[REDACTED] Direction finding operations were unsuccessful primarily due to the rugged Korean terrains and equipment malfunctions associated with the mobile operation.

Non-military North Korean communications targets were first intercepted in 1952. Internal civil communications, which in many respects resembled our Western Union, produced plaintext messages passed among major North Korean cities and

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

industrial complexes. These messages contained a large variety of subject matter ranging from personal messages to coal, lead, zinc, and other mining statistics. In addition, order of battle information was derived when these messages were passed among members of the military forces.

Intercept of South Korean targets was initiated in June 1953, when South Korean President Syngman Rhee released approximately 25,000 prisoners without advising U.N. authorities. South Korean military, navy, air, and police communications were very closely monitored, particularly whenever President Rhee threatened to take unilateral action against North Korea. This threat action delayed the signing of the truce agreement for at least thirty days, until July 1953.

Since open hostilities have ceased and the situation has become static, North Korea continues her efforts to improve communications security. There has been further sophistication of cryptosystems and rigid adherence to communications security procedures. The use of radio communications has decreased, while the use of landlines and courier services has increased.

A SIGINT effort which began with North Korean forces crossing the 38th parallel on 25 June 1950, and developed to the point where valuable and useful intelligence resulted, has finally, with the conclusion of the war, reverted to a quiet peacetime problem. However, despite recent peaceful overtures between North and South Koreans, the North Koreans remain a well trained and well equipped military force with Chinese Red volunteers sitting just across the Yalu River.

Not only does a SIGINT requirement exist today, but SIGINT takes on a more significant role during peacetime situations when communications security is at its peak. During periods of open hostilities, the mobile situation tends to lessen communications security and offers the SIGINT producer a variety of intelligence sources.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

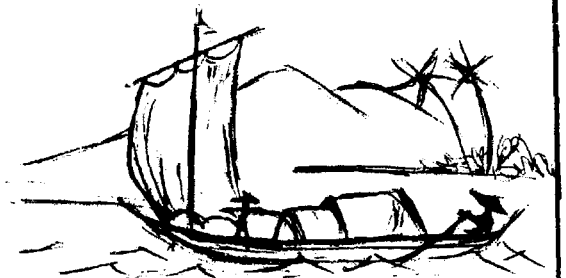
東洋의 山  
이 한 직

비 켜 마른 어깨가  
抗議 하는 양 날카로운 것은  
솜 꺾 앓고는 못 참는  
애 달픈 天稟 을 타고난 까닭 일꺼  
다  
激한 噴火의 記憶을 지녔다  
그 때는 어린 대로 심히 慍해  
볼 수도 있었기 때문이다.  
植 物 들은 해마다 헛되히  
뿌리를 뻗었으나  
끝 내 森林은 이루지 못하였다  
지나치게 倏 愴함을 겪고  
나면  
오 히려 이렇 게도 마음고요  
해 지는 것 알 까

## THE HILL OF THE ORIENT

YI HAN-JIK

THAT MY BONY SHOULDERS ARE SHARP  
AS IF IN PROTEST  
PERHAPS IS FROM THAT IMPATIENT  
TEMPER OF MINE  
WHICH SEES AND MUST ACCUSE.  
I CARRY MEMORIES OF VOLCANIC  
VIOLENCE;  
FOR THEN I WAS FREE TO BE FURIOUS.  
MY PLANTS HAD ROOTS, IN VAIN,  
EVERY YEAR  
AND NEVER GREW TO BE A FOREST.  
IS IT BECAUSE I HAVE WALKED  
THROUGH TOO MANY CRUELITIES  
THAT I AM IN SUCH QUIETUDE?  
I HAVE NOW NOTHING TO INSIST UPON.



~~TOP SECRET UMBRA~~

이제는 固執 하여야 할 아무  
主張도 없다

지금 山기슭에 "부주카" 砲가  
震動하고

共産主義者들이 낯설은  
外國말로 喊聲을  
올린다

구리고 實로 믿을 수 없을 만큼  
손쉽게

쓰러져 죽은 善意의 사람들

아 그러나 그 무엇이 나의 이고요  
함을

깨를 일 수 있으리오

눈을 꼭 감은 채

나의 表情은 그대로 얼어 붙었나  
보다

微笑마저 잊어버린

나는 東洋의 山이다

AT THE MOMENT

THE HILL-SIDES SHAKE FROM THE  
BAZOOKAS;

THE COMMUNISTS RAISE SHOUTING  
IN ALIEN TONGUES;

AND THOSE GOOD-WILLED PEOPLE  
HAVE FALLEN SO EASILY

THAT I CAN HARDLY BELIEVE IT.  
BUT, NOTHING CAN DISTURB ME OR  
MY QUIET NOW.

WITH TIGHT CLOSED EYES,

THE ICE OF MY EXPRESSION FREEZES  
HARD.

I, WHO EVEN HAVE FORGOTTEN HOW  
TO SMILE,

AM THE HILL OF THE ORIENT.

TRANSLATED BY KIM JONG-GIL

道

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

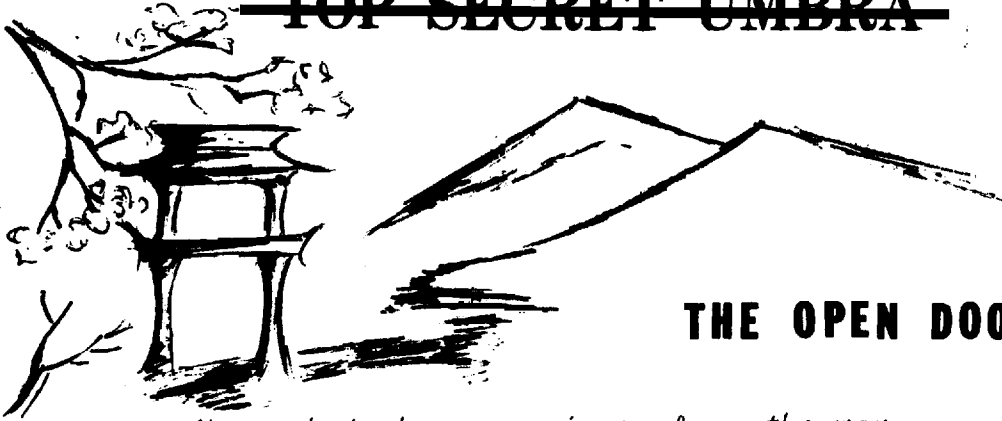
Transposition is.....

Our previous example of transposition involved a diagonal and blank cells. This is a simpler but still an intriguing version. Can you recover the key and the plain text?

ETNNS	CETAH	LIIAA	IWROX	ELEST
HEEEE	LAASI	CUTRB	ESVIF	SUAWH
BOYRL	SDPDM	UDISE	TOWMT	IYYVE
SSTFL	HPMUD	TNWRH	PSELH	ISFOI
LOMCR	NUIVT	LTOCE	TELANG	USOEE
NNXMA	BTOAN	HTIOS	CIWNI	XICNG
MLOTA	XFBPE	NHHER	LOPEB	LESEP
EREED	CEIEN	EIONT	LSIEN	OIERA
RICOO	OTTOO	MANUO	ITOXI	LTELA
TOAVE	XOAI F	EYAEN	OTOLP	MABOM
XEAEN	OCEAX	AEFEA	UXLRT	NIOOQ
XNRTP	IRIRE	NEFEX	LTXTE	ONHIT
FOOUR	EHQOO	HORUC	GNXEO	PCOND
RCRHD	BOURN	IGKXN	MHOEV	TESHT
RUTWD	ETNHI	NMLED	EURUA	CEDHA
IROGE	TGSDM	BIAXL	TETEV	EOAFB
MEXIY	MEHHN	ECHSA	NNRAM	TPTEH
RWECI	TCNTW	CXDDR	MNIRG	NWITN
AYEXC	EAGAF	FEWOL	XVWLD	ESONS
DHMNR	EQXAE	NATIG		

Solution in the next issue.



~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605**THE OPEN DOOR**

*We seek to be companions along the way.  
 The lantern which we carry is not ours.  
 The spirit which we share is contagious thought;  
 The knowledge which we gain, an illuminating torch  
 And all who seek may perceive and learn.*

*-The Concept of Dragon Seeds*

SIGINT SUPPORT ON THE ECONOMIC FRONT

by William Hunt, P2

When I was asked to write an article on SIGINT support to economics, it occurred to me that there was a feeling among certain personnel that the problem in NSA was something new. Most of us know that economic intelligence production in NSA is not new. I think it would be useful, though, to try to anticipate what changes in processing priorities will result from the statements of the United States Government regarding an increased emphasis on our economic posture, involving the placement of this country in a more competitive position vis-a-vis other major trading countries of the world and (a still more readily understandable consideration) the continued high value of our currency.

It is true that the emphasis in the past has been on military-type economics (which includes the production of weapons, weapon systems and hardware, the testing of new weapons, delivery of new weapons and related supplies to their national units and to foreign collaborating countries, etc.) and specifically on the ability of Communist Bloc countries to prepare for and sustain hostilities against the United States and its allies. It can be readily seen that almost any aspect of a country's economic status would contribute to the knowledge of its military capability. It can be concluded, therefore, that economic information from SIGINT has always been high on the mission of NSA. Priorities from time to time

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

have changed, depending on the requirement for this information and the general resources available. Generally speaking, priorities affect the scope of collection, the depth and detail of analysis, and the frequency and timeliness of reporting.

In August of this year, G Group decided to take a look at its readiness to respond to an increased interest in economic SIGINT. Since G produces most of the non-military type of economic SIGINT, and since this category is the most likely to be affected by an increase in the priority of economic intelligence, Chief, G Group established an "economic coordinator" as an advisor to look into the whole of the G Group economic SIGINT problem, including requirements, collection, processing, and reporting, with a view to being in a position to respond to any changes in the general G Group priorities system. A study staff of up to six personnel was envisaged to undertake this project. A basic charge to this staff was to study the problem but not to become involved in operations; its activity was to be confined to study--to probing the general problem area and reporting on the ideal organization within G Group to cope with the potentially increased emphasis on economic SIGINT, if such should be required.

The writer and one additional intelligence analyst have been studying this problem since August, and have just completed an interim report on the status of G Group and some recommendations to improve the G posture to meet the anticipated challenge.

Considerable progress has also been made in the customer community, including the rejuvenation and enlargement of the USIB Economic Intelligence Committee and the establishment of a sub-committee to deal with economic requirements. At this writing, a new Assistant Secretary for Economic Affairs has been named at the State Department (Mr. Casey), and Mr. Schultz, Secretary of the Treasury, has been given responsibility for over-all coordination of U.S. economic affairs.

With the exception of piecemeal, *ad hoc*, one-time requirements, no major SIGINT requirements demanding commensurate resources have been levied on NSA beyond the normal and mostly military-type economic requirements discussed above. Possibly some reorientation of the priority and/or processing of existing requirements will be forthcoming, and possibly there will be totally new requirements with emphasis on specifics and on more

~~TOP SECRET UMBRA~~

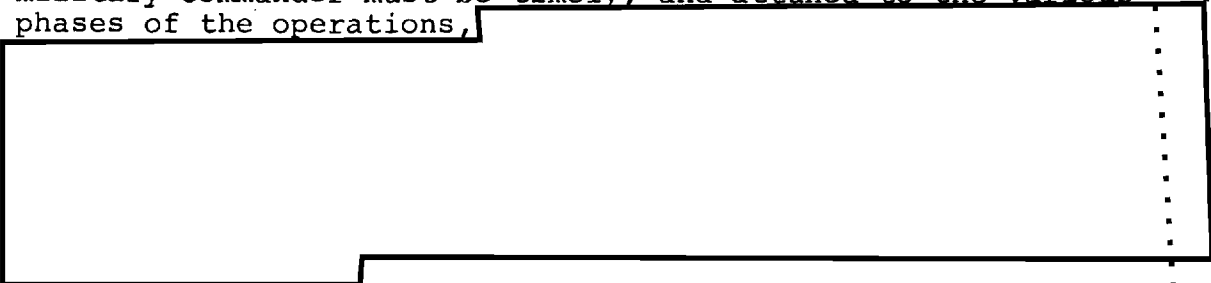
EO 3.3b(3)  
PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~

timely reporting. It is conceivable that some de-emphasis may occur on the traditional problems, and that this will entail a reorienting of scarce skills, i.e., linguists, research, analysts, report writers, etc.

Hour for hour and pound for pound of intercepted traffic, diplomatic communications provide the best yield of economic information, whether the traffic is encrypted or plaintext. It is for this reason that no let-up in the intercept and processing of diplomatic traffic should be considered in order to increase the output of economic SIGINT.

We must, if anything, increase the flexibility of processing and reporting such traffic. The nature of the economic problem will be such that we may be required to organize, process, and/or report in many forms, with timeliness an extremely important factor. Just as tactical support to a military commander must be timely, and attuned to the various phases of the operations,



promise to yield mass volumes of such data, which will require mass machine scanning, etc. These processing techniques are currently being tested, and it is hoped that the increase in human effort can be kept to a minimum; however, it would be unrealistic to hope that no increase in linguists, analysts, or report writers will be required for an increased economic effort.

A de-emphasis of traditional military problems because of a relatively relaxed international atmosphere will undoubtedly permit the reassignment of some personnel from these problems to the possibly emphasized economic ones. By no standard can we expect an increase in any resources of NSA in these times of stringent budgets. We must be looking for better machine-processing methods, machine outputs designed to meet customer

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

requirements with the minimum of narrative, information banks which can be readily queried, etc. Only by the adoption of these techniques can we ever hope to cope with the increased volume of material and the possibly increased requirements.

In addition to providing [redacted] to the traditional Departments and Agencies, all of whom have supporting intelligence production organizations, we must consider new members [redacted] organizations that may not have SIGINT analytic support integral to their organizations. In these instances we must plan for providing the required support in easily readable form, devoid of SIGINT jargon and intelligible without recourse to special interpretation.

*NOTE: This article appeared in the January 1973 issue of Keyword and is reprinted here with the kind permission of the Editor of Keyword and the author.*

*In view of the changing relationship between the United States and Asian countries, particularly the Peoples' Republic of China, one may expect an increased interest in economic SIGINT from B target areas.*

\*\*\*\*

"Shall I tell you what knowledge is? It is to know both what one knows and what one does not know."

----Confucius

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

THE GROUND ZERO APPROACH TO LANGUAGE ANALYSIS

by Dan Buckley, B61

The "ground zero" approach to language analysis is the mechanical application of language skills (at whatever level of competence) to a particular target on a day-to-day basis, without regard for anything that happened yesterday and without concern for what may happen tomorrow--or beginning each day at "ground zero." It's easy, comfortable, and best of all, it's safe. Like most people, linguists have security blankets. Among their favorites: "I know what it says--you figure out what it means." This is closely followed by the nonsensical replacement of foreign words with English equivalents (more or less). For example, in Vietnamese this results in "dropping 200 pounds sterling bombs" for *nem bom 2000 bang anh* or "active activity" for *hoat dong tích cuc* rather than "2000 pounders" and "positive action." Does "ground zero" then become *mat khong*?"

At any rate, the "ground zero" approach is more than safe; it is irresponsible and ineffective. You can't work traffic successfully with such a method because you can't know what is abnormal (reportable) if you don't know what is normal; and you can't know what is normal if you know only what is happening today. You have to know about yesterday and care about tomorrow--and then you have to do something about it. Here are some things you might try to cure the "ground zero" syndrome:

1. Constantly improve your language capability. Don't use cipher traffic to do this unless you never read it as part of the job. If cipher traffic is your field, read plaintext for practice. Newspapers are even better because while reading traffic won't help your vocabulary and structure problems much, newspapers will; and the newspapers will help you to read traffic.

2. Have your translations checked occasionally, especially one that you consider well done. It doesn't do much for the ego sometimes, but it is an effective learning method. Don't be embarrassed if it's not as good a translation as you thought--you really need from three to five years of varied experience to be a highly qualified translator.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

3. Don't be lulled (self-satisfied?) into thinking of yourself as a "hotshot liny" because of practiced facility with a particular group of traffic. Most VE-100 grads could learn to read and work artillery traffic in a week, so you might want to ensure that you aren't confusing expertise with familiarity. Try not to spend more than a year at the same desk, or rather, with the same group of traffic. You ought to make some effort to expand your qualifications, keeping in mind that undeveloped people tend to make a significant contribution to their own undevelopment.

4. Practice writing out translations in good English. The best translation is one that reads as though it was never in any other language. *Nha cua anh Tam* ought never to come out "the house of Mr. Tam"--why not "Tam's house?"

5. Don't mistranslate anything, ever. Sooner or later you are going to have to come to grips with a fact of the translator's life: there are some things you don't know. Socrates had something to say once about the really smart guy knowing the limitations of his knowledge.

6. Be specifically aware of everything that happens in your traffic and generally aware of what's going on about you. The "liny" working the traffic is the duty expert--make no mistake about it. If you don't know the little things that happen every day and their relationship to one another, there is probably no one who does know.

7. Keep records. That's the answer to the question generated by paragraph 6. Keep records on OB, personalities, locations, and events at least on a system/unit basis. It helps you to keep track of what's going on, helps with crypt-system identification, and in the event of your untimely departure it helps the next guy get snapped in that much faster.

8. Learn an effective writing style. That really may not require a major change but something as apparently insignificant as switching from passive to active voice: "NVA forces in southern Laos will launch a major offensive..." rather than "It was noted that a major offensive is to be launched by NVA forces in southern Laos..." If you need help here, get it from any of the senior language analysts. Most of them make at least \$15,000 a year and you can help them to

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

earn it. Seriously, every one of them will be glad to help you, and I can honestly say that I don't know a single man or woman among them who would feel that you were imposing.

9. Get out of the "bubble." Language is not an end in itself; it is a tool--nothing more, nothing less. It can be used in breaking crypt-systems and recovering comms nets, just as C/A, T/A, and reporting are tools which can help the linguist. The linguist who operates in the "language bubble" is almost doomed to mediocrity and a performance at the "ground zero" level.

Finally, you ought to be asking yourself whether you are any better as a language analyst than you were last year. What language contribution have you made to your section/branch that was not levied upon you by someone else? Are you operating at somewhere near maximum capacity? Is 100 messages a week truly the limit of your capability? As resources diminish, someone else is likely to ask those questions--and they are legitimate. If "ground zero" is your location, there is no better time to move than now.

\*\*\*\*

ເຈັ້ນ ມີ ຜູ້ ສາວ ຈາກ ບ້ານ ບ້ານ  
ຜູ້ ນຸ່ງ ກະໂປ່ງ ຫລາຍ ສັ້ນ ສັ້ນ  
ລາວ ພົບ ທະຫວານ ມື້  
ຜູ້ ເຈັ້ນ ເອົາ ເອົາ ເອົາ  
ແລະ ດຽວ ນີ້ ເຂົາ ບໍ່ ວຽງຈັນ ຫວານ

There was a young lady from  
Ban Ban  
Who wore her skirts very  
san san.  
She met a G.I.  
Who gave her the eye  
And now they live in sweet  
Vientiane.

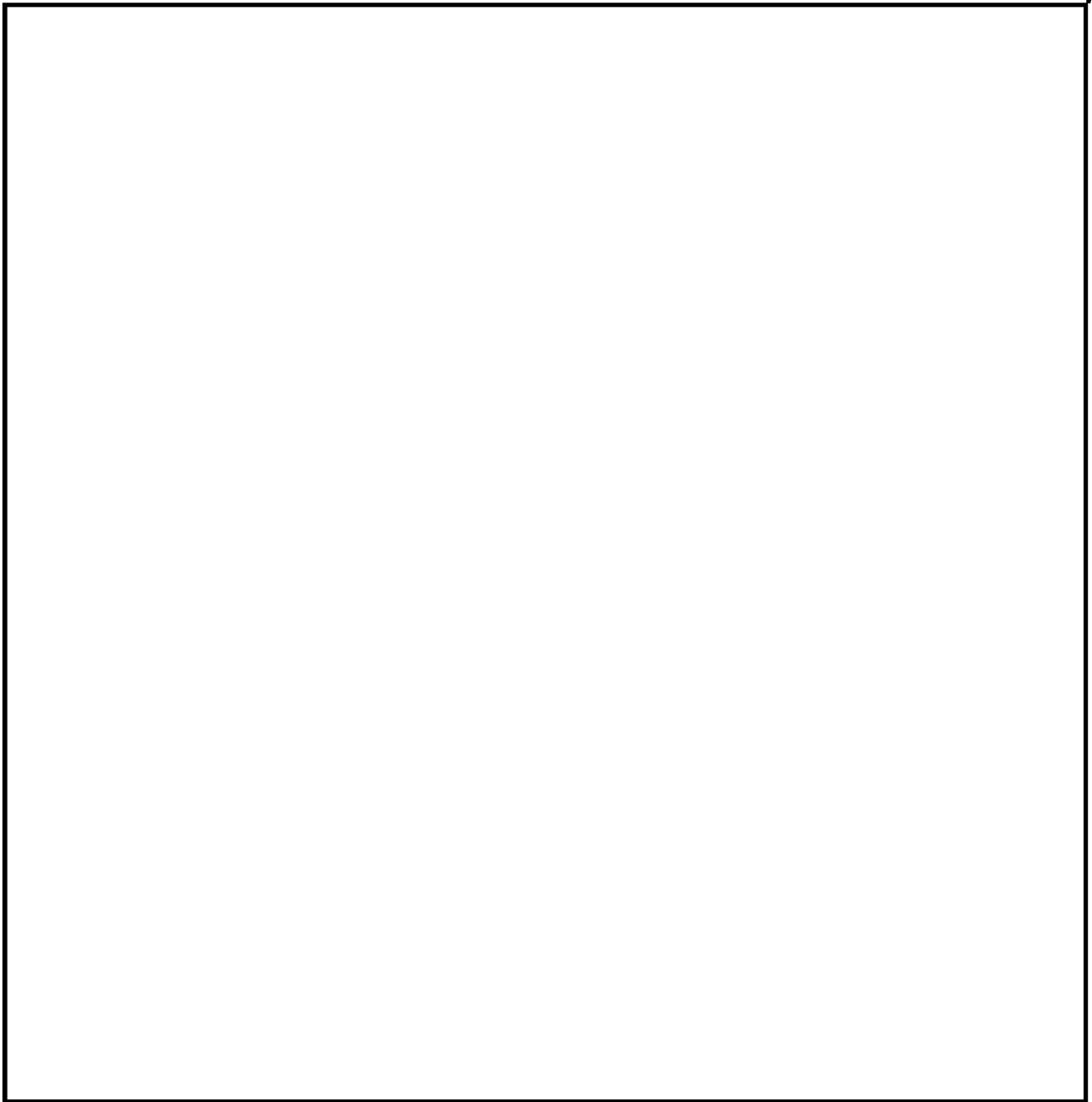
---Doug Perrit, B12

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EXPLOITING THE BUST

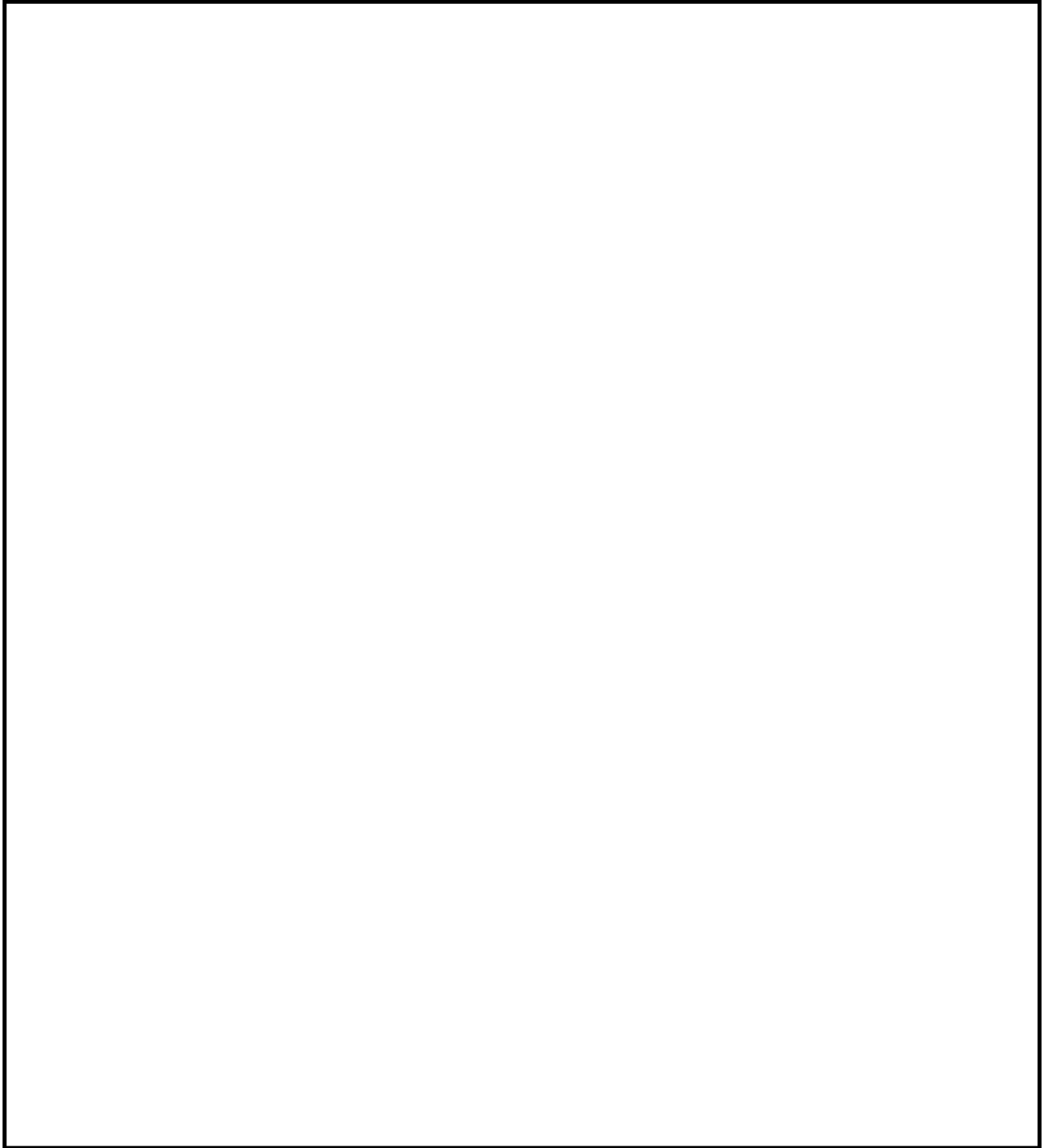
by Kenneth Miller, B43



~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

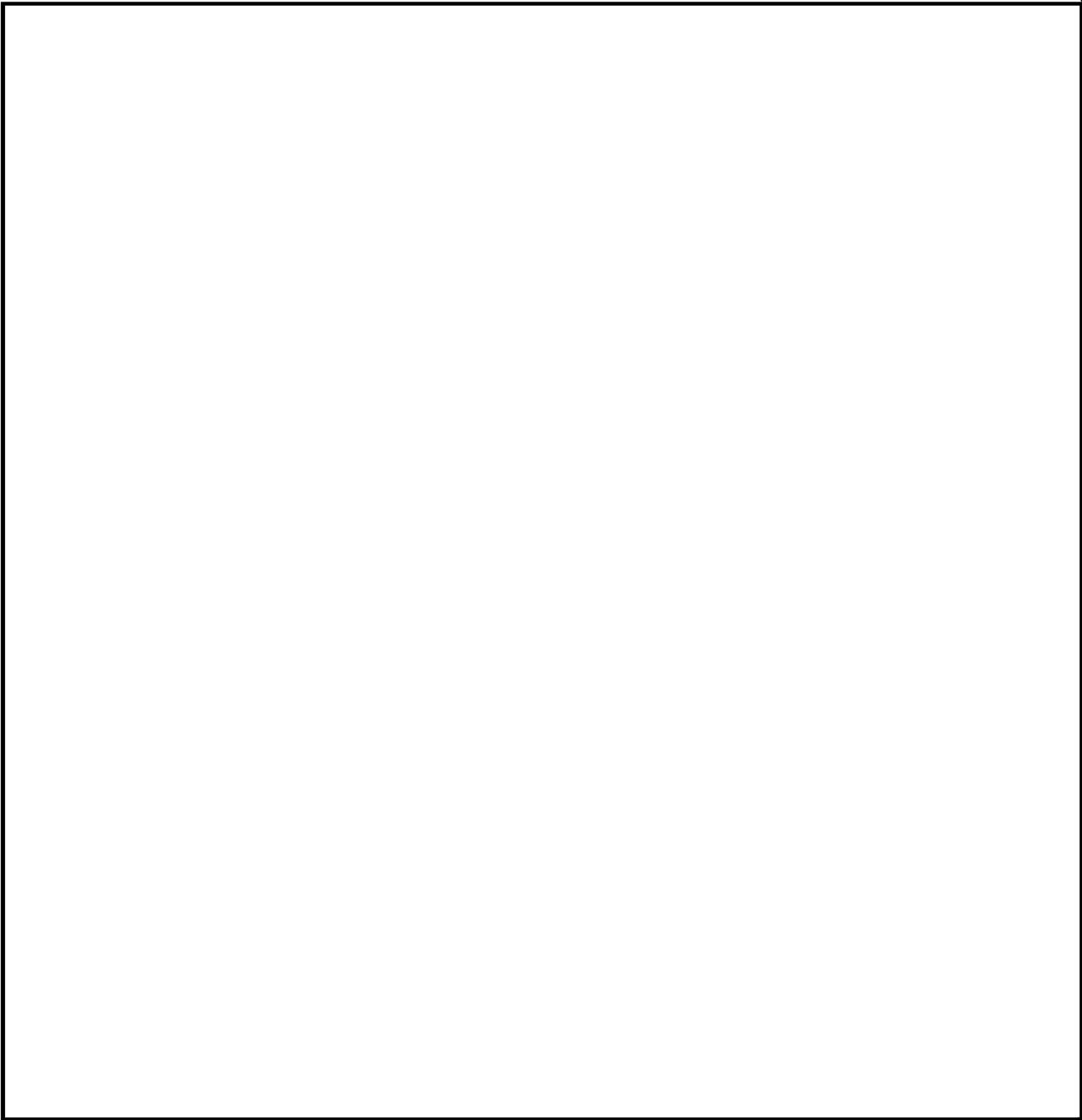
~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

ONCE MORE THE TSR

by Jane Dunn, B45

The TSR or Technical SIGINT Report is, according to the pertinent NSA Publication Manual, "a vehicle for authoritative presentation of significant analytical results which are sufficiently well established to convey a technical conclusion or theory and which may be used as a basis for further analysis and/or product reporting." I believe that this definition ignores a very important aspect of the TSR--the quality of its writing.

We have all heard the pleas for technical reports to document analysis so that vital technical and historical information does not leave the organization with the departing analyst. High-level concern about deficiencies in our report writing has resulted in an explosion of NSA writing courses and in the requirement for evaluation of English competence in the performance appraisal of employees above a certain grade level. Unfortunately, the number of well written technical reports does not seem to have increased in proportion to the attention given in recent years to the "English" problem. Although a poor report is probably better than none (even if the ultimate reader has to do some textual analysis to discover what the writer is trying to say), there is little excuse for poor writing in an agency like ours where the average level of formal education is exceptionally high.

As bad money drives the good out of circulation, so poor writing overwhelms the excellent and drives it underground. We become so accustomed to the dreary procession of cliché, jargon, and stereotype that we risk losing our power of discrimination. Standards slip lower and lower until what has been described as "illiterate garbage" becomes the accepted norm, and only the occasional appearance of a well organized, informative, literate piece of technical writing reminds us that we can do better. But how? Perhaps the first step in the steep climb toward excellence is to take a good look at some of the technical reports we have ourselves produced or read.

Rarely does a SIGINT target organization send or receive a cipher message; encrypted traffic is transmitted by some entity in communications with another. Nor does any monitor intercept such a message; encrypted traffic is observed being passed by

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

subject entities. A Polvetzian regiment seldom uses PQMR-127 for daily strength reports; a PQ regimental level military entity is presently utilizing cryptosystem PQMR-127 for daily reporting of personnel strength. In fact, nothing is now used; it is presently being utilized. Such overblown verbiage is hard to swallow the first time it appears; when it is repeated in all appropriate slots in a stereotyped format, it becomes downright sickening. Is it any wonder such reports pass quickly across the desk and into the burn bag or the darkest corner of a file drawer?

From the evidence of published TSR, the prospect of writing a technical report must terrify many analysts. Faced with producing such a report, the writer scurries to the files for an earlier document which he can republish after substituting more current dates and adding a handful of new details. He thus has a security blanket, but does he have a report? The published result is not the product of analysis but the regurgitation of an analyst's card file. The nadir of technical reporting is to publish a printout of an IBM deck under a TSR number and title.

Another security blanket for the technical reporter is the check-off list designed as a memory aid but too often used as the incorporated outline for a TSR. Relying on such a grocery list leads to the deadly practice of making some entry under each heading even if that entry is "Nothing to report" or "Not applicable." Both the "update" and the check-off list allow the writer to withdraw, however ungracefully, not only from taking responsibility for analysis but also, one is tempted to conclude, from thinking.

Guidelines for effective writing abound. They cover the field from "correct" grammar and punctuation to hints on writing style. The analyst who seriously wants to improve his technical reports will find that he gathers dividends from an investment of time and, if necessary, money in using such aids. At the very least, the investor will avoid the danger of having his conclusions dismissed as unreliable because the reader equates poor writing with fuzzy thinking.

~~TOP SECRET UMBRA~~

# ~~TOP SECRET UMBRA~~

## CRYPTO-SCRAMBLE

*Ray Titus*

Unscramble each of the four numbered crypto-scrambles, placing one letter in each space, to form four words or names, each of which fits the definition to its right.

1. O X O P I A N T I T L E  
\_ O \_ \_ \_ \_ O \_ \_ \_ \_ \_

Production of information from messages that are encrypted in systems whose basic elements are known.

2. E N P A B S T S O I L O  
O \_ O \_ \_ \_ \_ \_ \_ \_ O \_

Used to determine causal or random repetitions.

3. N A K K Y B E  
\_ O \_ \_ \_ O \_ \_

File of available keys.

4. A R T M E N O T E  
\_ \_ O \_ \_ \_ O \_ \_ \_

Group of 4 digits

Now arrange the circled letters to form the cryptoanswer suggested by the cartoon at the right.

Print CRYPTOANSWER here :

Sounds like the confessions of a skyjacker.



Answer on page 37 .

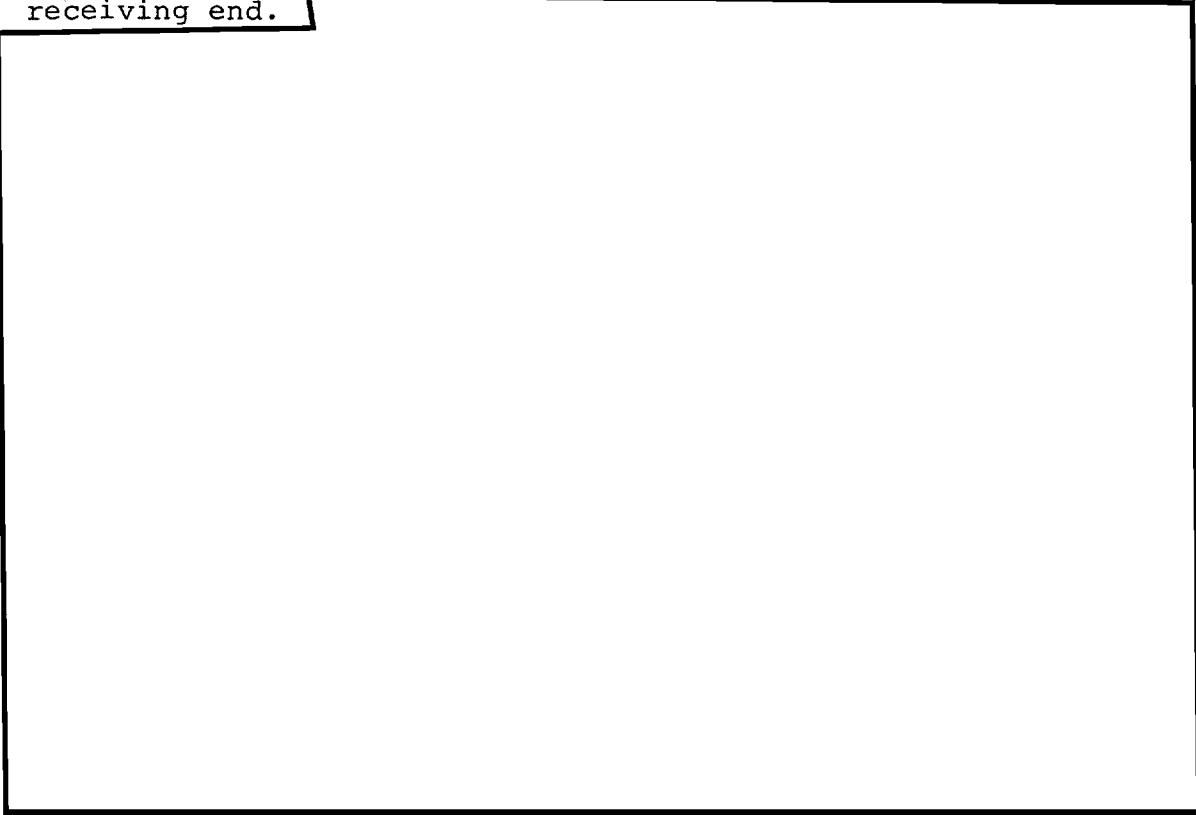
~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

HOW ABOUT THE OLDSMOBILE M?

by Thomas Wood, B34

At the start of the "air war," when the bombing of North Vietnam began in earnest, the neighbors to the north were concerned that they might become involved---on the receiving end.



Having reached the correct solution (albeit incorrectly), we saw no reason to advise the customer of any anomaly in the text of the published translation!

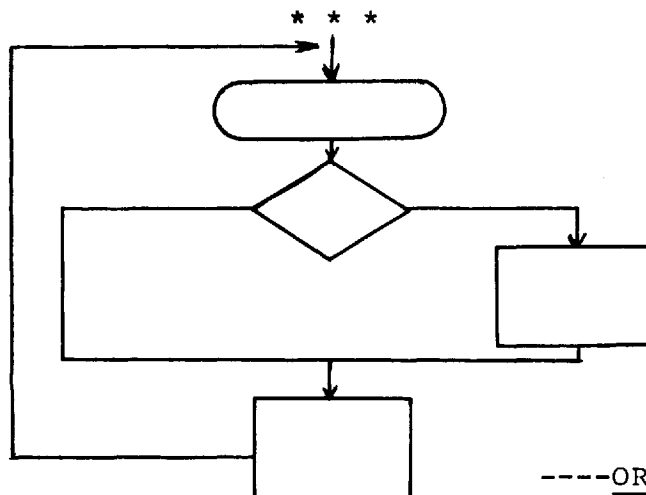
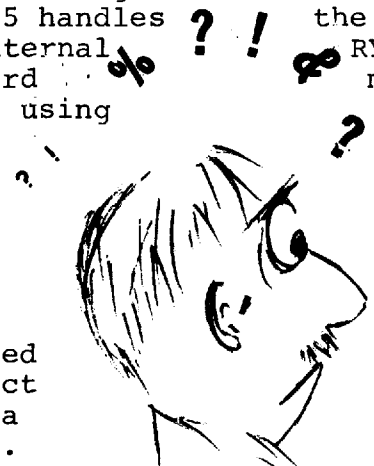
~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

STANDARDIZATION????

by Russ Myers, B12

Three data preparation media to ready messages for insertion into the FASTRAND drum file are available to bookbreakers using Project TREES on RYE. They may punch the messages onto ASR-35 paper tape in ASCII 7-level coding or onto cards via the IBM 029 keypunch in EBCDIC coding or the IBM 026 key punch in FORTRAN-H coding. The ASR-35 handles the translation of ASCII-coded paper tape into internal RYE FIELDATA coding; however, a "translation" card must be provided with card input. If you are using a SORBAN card reader, without its own internal coding, you need only provide for translation from EBCDIC card code or FORTRAN-H card code to RYE internal FIELDATA code, as appropriate. However, if you use a UNIVAC-1004 "translation" card will facilitate the conversion from the UNIVAC-1004 oriented XS-3 coding to FIELDATA coding. The Project TREES program, OLIVE, will conveniently copy a RYE FASTRAND message file onto magnetic tape. The tape will be BCD coded. I suspect something was lost in "translation" when my sponsor did not recognize the special characters on the message file tape I provided him when he listed it on his Burroughs B300 outstation in BCL coding.



-----OR CONFUSION????



~~TOP SECRET UMBRA~~

-----B GROUP EXPANDS; NEW OFFICE ESTABLISHED. The Office of Asian Systems Development, B7, with Mr. Coleman Goldberg as chief, came into being 8 February 1973. This new addition to B Group will be responsible for initiating, coordinating, and implementing a comprehensive program for upgrading the PRC collection posture and improving the management of B collection assets.

\*\*\*\*

-----The revisions in the criteria for professionalization in several career fields are highlighted below for your information. If there are any questions, please contact your training coordinator or the Executive of the individual panels.

•Special Research: A written Professionalization Qualification Examination was instituted as of 15 January 1973. The oral interview will still be required if an aspirant scores between 70 and 80 on the PQE or at the option of the Panel if a score of 81 or above is obtained.

•Traffic Analysis: Effective 1 January 1973, the basic

requirements for certification in the Traffic Analysis career field are 1) high school graduation or certificate of equivalency; 2) a documentary report acceptable to the Panel; and 3) passing the T/A PQE which, beginning calendar year 1973, will be offered only once a year. This year, Part I will be offered in May and Part II in December.

•Signals Analysis: The revised criteria, published on 26 October 1972, differs in two ways from the old. The first is that maximum performance points have been dropped from 500 to 250 points; the minimum remains at 150 points. To obtain points in this category, a candidate must submit a technical or methodical report which presents either a signals processing or analytic approach or system conceived by the candidate, the results of such an approach or system, or the results of a signals or telemetry analysis effort. The second difference is that computer and physical science courses have been added to the list of related courses.

--By the way--the Cryptanalysis, Language, and Traffic Analysis Career Panels have been relocated to 3C051.

\*\*\*\*

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

----Did U Know? There is a "Hot Line" in the main NSA Building. YES--a 24-hour recording device is in operation in the office of the Senior Enlisted Advisor to the Director, NSA. The purpose of this "Hot Line" is to make available a round-the-clock method of helping the enlisted personnel stationed at NSA with any problems that cannot be resolved through normal channels. To use this outstanding service, just dial "IDEA" (4332s).

\*\*\*\*

----L14, the Transportation Office, has been conducting a series of surveys about establishing commuter bus services in various areas such as Columbia, Md., and Washington, D.C. Personnel willing to support those services or interested in initiating other services should contact the Transportation Officer, L14.

\*\*\*\*

----Congratulations to Virginia Valaki and her cohorts in G5 for successfully penetrating an



\*\*\*\*

----BLITZ COURSE ON RYE...The Cryptanalysis Department of the NCSch is offering a new course, called RYE Operations for Cryptanalytic Applications. CA-090 is designed to give the working cryptanalyst practical experience in using RYE effectively as an aid in solving cryptanalytic problems. The course length is two weeks, half-time. It includes detailed discussion and usage of 15 GUPPY programs. Prospective students should have a working knowledge of cryptanalytic terms and techniques (CA-100 level). The first class is being offered in March. For further information, contact the CA Department, 8025.

\*\*\*\*

----On 23 January 1973, the Language Career Panel held its first formal graduation ceremony in the Director's Conference Room, at which time 23 language interns, representing eight languages, received letters of completion of the intern program. Thirteen of the graduates also received Professional Linguist certificates.

Mr. Robert K. Hess, Chairman of the Language Career Panel, opened the ceremony with a capsule report of the Language Intern Program. He then introduced the Language Career Panel Members, Advisors, and Staff, former Executives, and

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Language Intern Sponsors. Dr. Louis W. Tordella, Deputy Director, addressed the graduates on the subject of language work at NSA. He was assisted by Mr. John J. Connelly, ADPM, in presenting the certificates to the graduates.

The ceremony was followed by a brief reception which featured sparkling punch and petit fours.

The graduates and the languages they represent are:

\*Daniel J. Allman, Japanese  
 [redacted] German  
 Carol Buschbaum, French  
 David G. Chizum, Russian  
 Donald H. Deitrick, Korean  
 \*David G. Dillard, Spanish/  
 Portuguese  
 Gerald L. Everett, Spanish  
 \*Linda L. Franklin, French  
 \*Richard L. Gibson, French  
 \*Marjorie D. Hamlett, Spanish  
 Margaret K. Keirstead, Spanish  
 Terry L. Lyons, German  
 \*Carole A. McGee, Arabic  
 \*William S. Olmsted, Russian  
 Veronica J. Palk, Arabic  
 \*Michael G. Pond, Russian  
 \*Martin J. Savalchak, Russian  
 Sheila B. Singer, Portuguese/  
 Spanish  
 \*Susan L. Smith, Arabic  
 Arlene M. Sullivan, Japanese  
 \*Joanne L. Urban, Spanish  
 Florence E. Wagner, Shan  
 \*Georgianne M. Weiser, Arabic

\*Graduated with Certification

\*\*\*\*

----Would you believe that G8 didn't find out until 27 February that B1 had relocated to FANX II from FANX III in October? There just ought to be a law!

\*\*\*\*

----Papers for The CLA essay contest can be submitted through 31 March 1973. Send three copies to Mr. C. G. Pritchard, Secretary CLA, B5111, FANX III. Prizes of \$100, \$50, and \$25 will be awarded at the Annual Banquet (date to be announced). The criteria for judging the contest are:

- a. Relevance to the cryptology of the subject and treatment.
- b. Interest of the paper to NSA professionals.
- c. Style of writing.

For security rules, consult the Technical Journal, Vol XI, No. 4, 1966. Papers that you have written concerning your regular assignment may very well be candidates for submission.

Don't forget the deadline date-- 31 March.

\*\*\*\*

----Keep 7 and 8 May open dates on your calendar. That's when the Institute for Advanced Technology (Control Data Corporation) is holding its seminar on Data Base Concepts in the Washington, D.C.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

PL 86-36/50 USC 3605

area. This seminar will provide management with a general understanding of data base concepts. In particular, management's role in the design and implementation of the data base will be addressed.

Other dates of interest are 25 to 27 April, when the same sponsor will hold its local seminar on Advanced Programming Techniques. The seminar, designed for programmers, analysts, and their technically oriented supervisors, will deal with philosophies and advanced techniques of computer programming. Ideas applicable to any machine and any programming language will be discussed. Special attention will be given to FORTRAN, COBOL, PL/1 and assembly languages.

\*\*\*\*

----The joint meeting of all members, past and present, of the TA, CA, LA, and SRA Intern Programs scheduled for 14 March in the NSA auditorium will be reviewed in the next issue. The guest speaker will be Mr. David Y. McManis, Chief of the White House Situation Room.

\*\*\*\*

----Smiles and Tears: We are happy to announce the recovery of two members of the *Dragon Seeds* staff: Ray Lynch, B44, from a heart attack, and Lorna Selby, B1, from an eye operation.

Victor Tanner, our Rewrite Editor, has turned in his red

pencil and is off again to Vietnam (his fourth or fifth tour). [redacted] formerly of the Press Corps, is enroute to the same destination.

\*\*\*\*

Solution to puzzle:

1. Exploitation
2. Poisson Table
3. Key Bank
4. Tetranome

Crypto-answer:

Plain Text

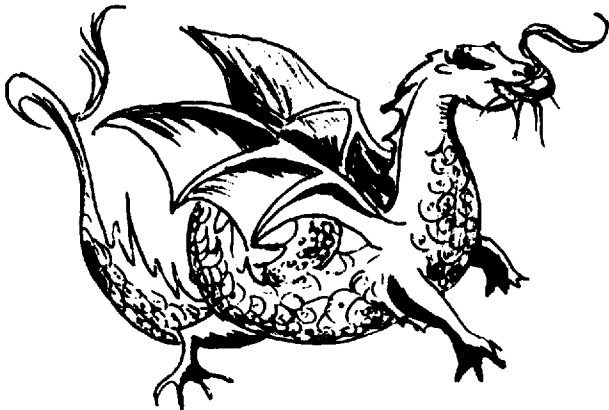
\*\*\*\*

TUNNEL VISION

----As glaucoma can lead to total blindness, ignorance of other disciplines can lead to total analytic failure. The cryptanalyst who ignores station identification and traffic laning deprives himself of a most valuable tool and can insure smearing of any statistical values which could give the system away. The traffic analyst who ignores crypt discriminants and indicators similarly throws away clues to station ident and callsign system structure and usage.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



ASK  
THE  
DRAGON  
LADY

TO: Mr. Leon F. O'Meara, C5

Dear Mr. O'Meara:

The following questions were submitted to the Dragon Lady by B Group open-shop programmers. We are forwarding them to you with the hope that you and your staff of experts will enhance our enlightenment by supplying the answers.

1. For any programming application, the maximum result is attained by a Time Sharing Option (TSO). The programmer sits down, programs, debugs, and executes in what appears to be an on-line one-on-one environment. Time Sharing Systems are used to service many programmers at different locations. The RYE System is the closest thing NSA offers to a TSO. APL is a real TS system but, because of restrictive file capacity and lack of resources, is not a practical alternative. The question, then, is: With all the resources--CPUs, ASRs, 2260s, and APL terminals--and a large debug workload, isn't it time for such a service to be made available to open-shop programmers?

2. "Re-inventing the wheel" is a cute phrase around NSA, and also a daily occurrence in the programming field. Why isn't there a readily available multi-volume set of program, machine, and system descriptions representing a central repository of information? Why isn't there an updating service for technical manuals which incorporates additions and explanations by the technical staff to further the dissemination of information?

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

3. There is more than enough work to go around. With that as a basic premise, wouldn't it be better to permit the programming staff to attack any problem in the language which suits it best, rather than introducing new languages of dubious value? Also, wouldn't it be logical to standardize languages across several machines (i.e., FORTRAN, IBM 370H, B6700, RYE, etc.)?

4. How is change effected? Is a more responsive mechanism than the Suggestion Program needed in the area of data processing? Are we afflicted with the "not-made-here" syndrome?

You can appreciate our reluctance to tackle these queries and can understand our urgent request for assistance. We would like to include both the questions and any rejoinders you may supply in our next issue.

DRAGON LADY, B03

Dear Dragon Lady:

I hope that the following will be adequate answers for your questions. Further clarification can be obtained from appropriate C5 representatives.

1. IBM defines time sharing as "the shared, conversational, and concurrent use of a computing system by a number of users at remote terminals." TSO (IBM's Time Sharing Option) is designed, according to available documentation, to provide a time sharing environment for terminal-oriented applications. It provides the user at a terminal with a command language with which he can develop, test, and execute programs conveniently; it also contains data entry, editing, and retrieval features. Time sharing jobs entered from the terminal (foreground jobs) share system resources with batch jobs (background jobs) that are being processed at the same time.

TSO appears to have numerous advantages for programmers and users in a terminal environment. However, there are several restrictions involving its use which must be studied. No single software package is the answer to everyone's prayers; TSO's apparent benefits are not without balancing drawbacks. Some OS

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

facilities are unavailable to foreground jobs; the execution of all jobs may be seriously affected if TSO is not appropriately "tuned" for our regular job mix; the monitoring of system use and performance becomes a highly complex job; and security problems--the needs for adequate data and program protection--are increased.

C Group is hoping to obtain, in early Spring 1973, an IBM 370/155. One of its principal uses will be the test and evaluation of TSO for use at NSA. We hope that by careful study and experimentation with different facets of TSO we will be better prepared to calculate its effects on our overall data processing efforts. We can then fit TSO into our systems with a minimum of upheaval and discomfort for users.

2. We agree that a great need exists for a central "library" of data processing information. Most offices in C Group maintain their own libraries in a more or less haphazard manner. The P2 Technical Library maintains several shelves of technical information concerning computer hardware and is an excellent source of generalized information on "what's available" in the marketplace.

Within C, C5 and C9 are attempting to create a computerized facility containing information about our own hardware systems. Hopefully, it will contain current information about the resources of a particular system, the locations and types of terminals, and the like. The problem becomes an obvious one, however, whenever the word "current" is used. Some decision must be made about who will be responsible for updating the file and how information will be filtered to that individual or organization whenever changes are required. It is not a simple matter.

Technical manuals are a different kind of problem. C9 attempts to make available the latest updates to IBM and Burrough's manuals. Information is supplemented by "User Bulletins" published by the C9 offices responsible for the various systems. C7 also publishes "Technical Bulletins" designed to make users aware of any changes which might affect them. Beyond this, C Group does not, at the present time, have the human resources to cope with a problem which is, admittedly, staggering.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

3. We believe that for any given programming application there are a variety of factors which should be considered in determining a preferred computer solution. Primary factors include the following:

(1) Accessibility of the data file(s) as input to the program on the preferred computer.

(2) Adequacy of the computer resources for the demands of the application.

(3) The needed type of user access to the computer environment.

(4) The programming language and associated compiler which best meet the demands of the application.

(5) Availability of the preferred computer resource for the specific application.

(6) Priority of the application in relation to other demands for the preferred computer resource.

Secondary factors which might affect the computer solution include the following:

(1) The availability of a programmer.

(2) The programming language repertoire of the available programmer.

(3) The presence of a computer which is not as heavily loaded as other choices.

A program for a manager of programmers is to minimize the impact of the secondary factors, particularly if they force an undesirable compromise on the primary factors.

To be more specific on the first part of Question 3, we believe that selecting the best programming language for a given application is a very important process and should be done in light of the above factors. C has a software division (C95, the Languages and Compilers Division) whose services are available to assist the user in this process. In addition, this division provides direct customer support for solving problems

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

in using a programming language or its associated compiler. A telephone call to secure extension 4745 will tap this service. We also believe that a programmer with a working knowledge of several programming languages and compilers can do a better job in matching an application with a language than he can if he relies solely on one or two personally favorite compilers. Further, we think it is desirable for the open-shop programming manager to know which languages and compilers are supported by C Group and, equally as important, to know why each one is selected for support.

Briefly, C supports those programming languages and compilers which can provide the best production service to the NSA community. More specifically, C95 currently supplies nine higher-level programming languages and 23 associated compilers on our general purpose computers. All of these are proven, production grade resources. C95 is available to provide information for parties interested in specifics. To our knowledge, we do not "introduce new languages of dubious value." C9 employs a careful and critical review process before introducing a new language or a new compiler to the user community for production purposes. Part of this review process is to seek and consider the views and requirements of the user community.

To address the second part of your Question 3, an analysis of FORTRAN on the family of NSA computers was performed in 1967/68 with the objective of standardizing across the board. We discovered that the task would have been formidable for two primary reasons:

(1) As a language, FORTRAN is not rich enough to assure compatible meaning on different kinds of computers.

(2) No two of the FORTRAN compilers used at NSA are built with the same compiler technology.

Further elaboration can be found in an article, *Program Transferability*, in the *Proceedings of the NSA Network of Computers Conference, 1968 (NOC-68)*. A more recently published report titled *C95 Technical Bulletin No. 35, FORTRAN COMPARISON*, March 1972, is also available. To respond to the need for a standard programming language, we are building the NSA BETA language and compilers that are designed not only to avoid the above FORTRAN problems, but also to provide an algorithmic capability well suited to the needs of the open-shop cryptologic programmer.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

4. The problems of effecting change vary according to the size and complexity of the applications software system involved. If the software is a single purpose application system of moderate size, speed of change is mostly dependent on the availability of manpower to make the change. If, however, the software system involved is a large general purpose system such as KAY or GENED, there are often extremely difficult technical problems in either modifying or adding to the system. For example, one of the GENED problems which beset us for many months was the limit on the size of the error file. When the allowable file size was exceeded (an altogether too frequent occurrence), the system could not process any more data. A program change to expand the error file size seemed to be a simple solution, but detailed investigation by the software specialists who knew the system best showed that this seemingly simple change had cascading effects which would have necessitated a complete rewrite of the system. This investigation, in addition to studies of alternate solution, took weeks to accomplish. There was no "not invented here" syndrome in this problem; it was simply a very difficult technical problem that took a long time to resolve.

This example is indicative of the difficulties of making apparently simple changes to a complex system. There are, I am sure, examples of desirable changes to comparatively simple systems not being made because of the NIH syndrome. The best way to resolve this type of situation is for the line manager in the analytic area to discuss the proposals with the line manager (at Division level) in C5. A valid requirement or a worthwhile proposal should not be allowed to die at the analyst-analyst level. Managerial review is essential in these cases.

\* \* \*

*The Dragon Lady offers her humble apologies to Piqued, whose question in the December issue was unanswered...a composition error. In correction, she submits the following.*

Many people have asked "Why the TACP does not accept applicants for the T/A Intern Program if they have had more than two years cryptologic experience?" The selection criteria referring to experience states, "Must ordinarily have at least one year of T/A experience at minimum GGD-07 or E-5 level; however, must

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

not have more than two years of cryptologic experience at GGD-07/9 levels." (See O/M Subject: NSA Intern Program Vacancies, dated 28 August 1972.) I asked the Executive of the T/A Career Panel to comment on this. His views are:

"When people apply for the On-Board T/A Intern Program they are asked to submit a complete PQR with the other necessary forms. These PQRs are evaluated against the T/A Criteria for Professionalization. The general rule of thumb applied is that applicants with more than 600 points are considered well on the way toward the certification goal of 1000 points and certification. The accumulation of points over 600 is generally due to the experience factor or more than two years T/A experience as a GGD-07 or E-5.

"This is not, however, a hard and fast rule, since the TACP did accept an individual in the past for the program with more than two years T/A experience at the GGD-07 and 9 levels and an accumulation of over 700 points. The plan in this case was to arrange for an abbreviated program for this man. I say *was*, because he was also selected for an overseas position and chose to take that assignment in lieu of the T/A Intern Program.

"To sum up--each case is evaluated on its own merits. The Panel considers whether or not the applicant shows professional potential and weighs that against what the T/A Intern Program offers. The Panel is guided by the need to fill professional level positions in P; and in the selection process of on-board interns, the Panel tries to pick the best. Other selection criteria are listed in the announcement mentioned above."

\* \* \*

*If you are standing upright, don't  
worry if your shadow is crooked.*

----Fortune Cookie

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

## CONTRIBUTORS

DAN BUCKLEY first came to work at NSA as a Marine in 1963 after driving by the building 117 times, thinking it was a shoe factory. He was a language analyst and language section chief from 1963 to 1966, except when he was on TDY to Da Nang or Khe Sanh or Phu Bai or Chu Lai. He solved the Vietnam TDY problem in April 1966 by going PCS to Phu Bai, where he stayed until April 1967. On the way back to NSA, he stopped off at Fort DeWes long enough to finish first in a traffic analysis course of 44 students. In October 1970, he left the Marine Corps and came to work as a civilian for the Agency. He was certified by the language panel in March 1969 and by the SRA panel in February 1972. He is currently serving in an overseas billet in Southeast Asia.

RICHARD CHUN is Chief of the Language Support Branch, B443, a newly established organization which provides a centralized Chinese voice transcription and translation service for B operating elements. Mr. Chun joined NSA as a civilian in August 1962 after having served in the U.S. Army for 21 years. His introduction to cryptologic activities came when he was assigned to Headquarters, ASAPAC, as the first Korean linguist in the field. In June 1953, he headed the [redacted] problem at NSA and a year later, was assigned to ASA units in Korea and Japan, where he worked on [redacted] [redacted] problems until spring of 1967. His subsequent assignments include Deputy Chief of B27 (B11), Chief of ISPC-34 [redacted] Deputy Chief of B34, and Deputy Chief of B44, in that order.

JANE E. (BETTY) DUNN's connection with SIGINT dates back to WWII and covers targets from Japanese Military to CHICOM [redacted] with stops along the way for work on [redacted] [redacted] European Satellite, and Vietnamese Communist cryptosystems. She holds a B.E. from Duquesne University and was prepared to teach French in Pennsylvania high schools before she was detoured to Arlington Hall. Betty is a certified cryptanalyst, a tutor for the CA Intern program, an E.E.O. counsellor, and the biographic editor for Dragon Seeds. Since May 1972, she has been Chief of B45, the PRC [redacted] Division.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

WILLIAM G. FLYNN, B605, has been with NSA and predecessor agencies since 1952. Most of his more than 20 years cryptologic service has been spent within B Group, with limited assignments with P and D elements. A certified Special Research Analyst, he is currently assigned to the Intelligence Staff for all Communist Ground Forces activity in Southeast Asia. He has spent the past five years as the Special Project Officer for B6, and one of his projects was his involvement in the events of the Butcher Case.

WILLIAM HUNT is a graduate of the Marconi Radio Officer's School and completed a one-year college course in the Russian language. He has been continuously employed in cryptologic activities in the U.S. and overseas since 1940, serving in NSA and other cryptologic organizations in the signals collection, TA, and SRA professional fields. He is currently Chairman of the Signals Collection Career Panel. Among his varied line and staff assignments in NSA Production and staff assignments at the Agency level, Mr. Hunt was the editor of the NSA Daily SIGINT Summary. He is currently serving as a Special Assistant to the Chief, G, developing and coordinating SIGINT Economic Production Plans and Procedures.

KEN MILLER, cryptanalysis technician in B4331, has been with NSA since 1965, with time out for a tour with the Marines 1966-1969. During his first Agency assignment, he worked in B41 on the PRC callsign problem and then moved on to B432, the Research Branch of the Cryptologic Research Division. Here he has spent several years on the PRC high-grade Military [redacted] problems, to which he has recently added the Democratic Peoples Republic of Korea [redacted].

RUSS MYERS, B1203, joined the Agency in 1965 after serving four years with the USAFSS. Fifteen months of his Air Force tour were spent [redacted] one of the "garden spots of the world." At NSA, he spent two years in A8 as a traffic analyst and Russian linguist and then was selected for Class 10 of CV100. He moved to B1203 in 1968 as a cryptanalyst. Mr. Myers was a member of Class 24 of CA-400 and was detailed for six months to B42 under the B Internal Data Systems Training Program. He holds

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
EO 3.3b(6)  
PL 86-36/50 USC 3605

professional certification in traffic analysis, crypt-analysis, and computer systems analysis, as well as a BA in Government and Politics from the University of Maryland. Mr. Myers is currently involved in the development and management of several data processing projects for B12 problem areas.

GEOFFREY C. WOOD, Chief of B122, came to NSA in 1955 after a number of years in the Navy, serving in submarines and in the Amphibious Force. He was assigned in various capacities to the old ACOM organization; had a tour in the NSASCC, and represented B Group in the National Indications Center. He is professionalized as a Special Research Analyst and is treasurer of the Crypto-Linguistic Association.

THOM WOOD of B341 began his career as a Chinese linguist in 1958 when he volunteered to study the language, hoping for a shot at Monterey so he could stay close to his happy hunting grounds (Santa Cruz) and the lady he happily hunted (the current Mrs. Wood). After completing his language training--at New Haven--he came to the CHICOM [redacted] shop, where he demonstrated his immense potential by taking three months to make a single code recovery (D%). For the remainder of his short military career, Mr. Wood was a jack of all trades: intercept operator, "grass" translator, DF operator, and cryptpie. Mr. Wood converted to civilian status in the field of his demonstrated potential--cryptolinguistics--and there he has remained. He is a professional linguist who has served and collected souvenirs in [redacted] (a bottle of Plum), [redacted] (the phrase "show me the way to go home"), and [redacted] (Diana and Geoffrey--his two favorite [redacted]).

\*\*\*\*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

**STOP !**



IT'S

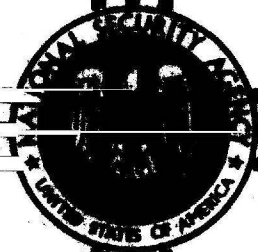
CLASSIFIED !!!

~~TOP SECRET UMBRA~~

~~TOP SECRET~~ *Mr. Callinane*

# National Security Agency

Fort George G. Meade, Maryland



JUNE 1973



# DRAGON SEEDS

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~



~~TOP SECRET UMBRA~~

This is *Dragon Seeds*.

There is fantasy, irony, and the bite of reality in the name. It speaks of the East. And, like the East, it suggests much, says little.

*Dragon Seeds* is both Mother China and her neighbors. *Dragon Seeds* is monumental and minuscule. It is the past and future. It begs for elaboration but gives none. In it are echoed softly slurred Mandarin, brittle Vietnamese, determined Korean. In it is the spectre looming over the Thai, Lao, and Khmer. It is frightening and friendly. It is uncertain.

Above all, *Dragon Seeds* is promise. It is fertile with ideas unbounded, to be cultivated with creativity and imagination. It is challenge. It is alive. It will be more than it is.

*Dragon Seeds* is yours. May it grow with you.

The Editors

~~TOP SECRET UMBRA~~

DRAGON SEEDS

Publisher

DONALD E. MC COWN, CHIEF B03

Managing Editor

Minnie M. Kenny

Feature Editor

Richard V. Curtin

Rewrite Editor

Victor Tanner

Executive Editor

Robert S. Benjamin

Biographical Editor

Jane Dunn

Education Editor

Marian I. Reed

Special Interest Editor

Ray F. Lynch

Composition  
Composition

Helen Ferrone  
Lorna Selby

PRESS CORPS

B11 Carolyn Y. Brown

B12 Philip J. Gallagher

B2 Dee Ensey

B31 Jack Spencer

B32 Jean Gilligan

B33 Louis Ambrosia

B34 Thomas L. Wood

B41 James W. Schmidt

B42 Peggy Barnhill

B43 Mary Ann Laslo

B44 Jack L. Thomas

B45 John E. Uzarek

B5 Nancy Fournier

B61

B62 Edmond J. Guest

B63 George S. Patterson

B63 William Eley

~~TOP SECRET UMBRA~~



Vol. 2  
Nr. II

June 1973

**TABLE OF CONTENTS**

Buddha Speaks.....1

GUPPY Mother Swims with TIDE     Peggy Barnhill 8

One Chance In Three.....Wm. Gerhard 10

Marketing Our Product.....Walter D. Abbott 18

The Open Door: The C Parallelogram or A  
Vietnam Cover Story.....Bee Kennard 22

Reflections On A Non-Random Bane.....  
Rodney Forbes 33

A Hitch-hiking Cipher....Mary Ann Laslo 38

Probing A New Technique...Dr. Marti Branstad 45

Seedlings..... 48

Ask The Dragon Lady..... 53

Contributors..... 57

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

B  
A  
D  
D  
D  
H  
A

RYE, AN EXTENDED CAPACITY REMOTE ACCESS SYSTEM

by Bernie Peters and Carolyn Palmer, PI

*"Nameless indeed is the source of creation  
But things have a mother and she has a name."*

---Lao Tzu

The RYE system was designed to handle a class of problems which was not satisfactorily dealt with by HARVEST or any other computer system current at NSA. These problems are characterized by small size, the need for immediate reaction, the need for intermediate human decision before final results can be produced, or the need for file-inquiry or information retrieval on a timely basis.

Some examples of these problems are:

1. Small jobs requiring only seconds on any computer, such as evaluating a message write-out on a single width. Any computer can compute the average IC and the IC for each column for any one reasonable width in seconds. If a fast, easily available procedure is at hand, the analyst will use it. If no quick method is available, the analyst may just write a few lines on a width and "try by eye," or may not attempt to prove or disprove the existence of width phenomena at all. The machine method is, in general, more thorough, more accurate and more economical, and leads to a higher percentage of solved systems.
2. Jobs with very critical response times. These are high priority jobs working in close support of a reading problem or a T/A development of CRITICOM significance.
3. Series of programs which are dependent on intermediate results for continued sequencing. The analyst considers these intermediate results before choosing the next program to be run, or before fixing on the parameters for the program.
4. Inquiry or information retrieval tasks (usually very input/output limited). Such tasks need the resources of a large computer with mass storage but cannot

SECRET

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

in themselves justify such a computer. RYE permits the efficient performance of relatively large information retrieval tasks while other processing is also being done and thus avoids "wasting" the time of a large computer.

All of these problems can be handled more economically by a centrally located large-scale processor to which a large number of stations have access than by scattering a large number of small-scale computers in various locations in the building. Since RYE is a real-time multi-channel device, the stations may all submit requests and receive back results without interfering with each other.

Outstations deliver requests and data to the computer via telephone lines (NSA grey phone system) and receive results back in the same manner. Depending on the amount of equipment involved, there are several classes of outstations. A general station consists of a model 35 Teletype only; a Class II station also has a BOSTIC, or high speed paper tape reader and punch device; Class I stations have Teletype and BOSTIC and, in addition, a lineprinter (UNIVAC 1004) and other high-speed equipment as needed.

### PROGRAMMING

The UNIVAC 494 is designed to be run on a real-time basis, accepting requests as the users choose to submit them and from all stations without interference with each other. It can manage itself with a minimum of operator intervention. This is accomplished by means of an extensive interrupt system and a sophisticated executive program.

Each object or worker program must be written with the following characteristics:

1. It is assembled so that it is completely relocatable in core and with regard to any facilities such as tape drives, drum storage areas, etc.
2. It uses the smallest possible amount of core area consistent with efficiency.
3. All input/output is accomplished by means of return jumps to the executive (REX).
4. No use is made of the console typewriter to request operator action, other than to complain about malfunctions.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

5. Large programs are segmented as much as possible consistent with efficiency.
6. Properly programmed error-checks are made to prevent program failure.

7. Programs are allowed to run only for a specified number of minutes (30 during the normal work-day, somewhat longer at night and on weekends and holidays). Hence an endless loop cannot tie up a large part of the machine for a long time. Also, long jobs have to be segmented if they are to be run on RYE at all.

With these rules and some additional conventions it is possible to provide prompt service to all the outstations.

#### PROGRAMMING PHILOSOPHY

The programming philosophy assumes continuous use. RYE operates 24 hours a day and 365 days a year, insofar as this goal can be attained. REX is able to interrupt any program at any time between the execution of successive instructions in order to service high priority interrupts, and the interrupted program is completely unaware of the happening. Outstations may submit requests at any time the Teletype is not already tied up with another job; in fact, all terminals may submit requests simultaneously. As soon as feasible after receiving an "end-of-transmission" signal from a terminal, the system will return a receipt giving the date and time of receipt, the internal job number assigned to the request, the first two lines of the request containing the priority (if any), program name, station numbers to which results are to be forwarded, and the requestor's name, section, and telephone extension.

Programs are run as soon as possible, according to the priority of the jobs awaiting scheduling. Priority is determined by the user, with the proviso that the user will not request a priority higher than the maximum official priority of the job. The user uses a lower priority if he does not want this run to interfere with his own more urgent tasks, if he wants the output held for delivery next morning or printed on the downstairs printer, or if this is the type of research job which should not interfere with any operational procedures but which he would like to have run in any slack time which may develop before next Monday. Only in exceptional cases, and with documentary

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

justification by the appropriate authority, is it permissible to run a job with a priority higher than its officially assigned maximum. This officially assigned maximum is based primarily on the amount of machine time, core space and additional facilities required by the program, but with some consideration of the overall importance of this particular task in the work of NSA.

Once a job has been placed in the scheduling queue, the program is placed in any available space in core as soon as it can be accommodated if the additional facilities required are available and if it is the first program in the queue which can be accommodated. Hence a small program may well be scheduled ahead of a larger job which has higher priority. Only in the case of a major emergency and on the direct authorization of the Chief A Group, Chief B Group, Chief C Group, Chief P1 or Chief P, are such drastic procedures as ditching jobs already in process resorted to in order to get a run started immediately. Hence, it is incumbent on programmers writing for projects with critical response times to use facilities as sparingly as possible, consistent with efficiency.

The executive runs as many programs "concurrently" as possible. This means that REX attempts to schedule as many of the jobs awaiting attention at one time as possible. Once a program has been assigned facilities and loaded into core, it can receive a share of the available running time. The oldest program in core is the first one to be considered for control. If it is awaiting the execution of an I/O request and has nothing to do, the next oldest program will be considered, etc. Thus, a small program, which "sneaks" into core in space too small for waiting higher priority jobs, may actually be completed before other jobs waiting in the queue with it are even started--and in what would otherwise be wasted time.

RYE periodically inventories the queue of jobs not yet completed to be sure that none is being unduly delayed, and takes corrective action to insure that all jobs are started within a reasonable time after their request, considering their priorities. RYE also keeps a complete log of all transactions and is able to answer queries from originators as to the status of their requests. For these purposes a unique job number is assigned to each request in strict order of receipt.

~~TOP SECRET UMBRA~~

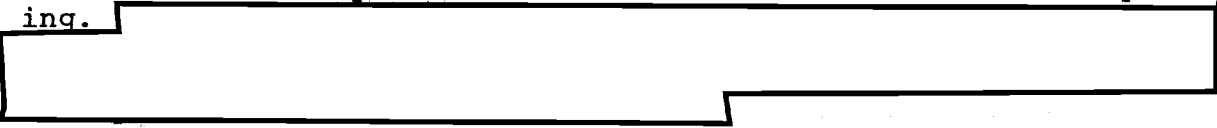


~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

### OUTSTATIONS

The basic outstation is a model 35 ASR Teletype. This permits communication into or out from the computer at a 10 character per second rate via keyboard, paper tape reader, punch and printer. This means that very long data tapes will take an appreciable time to input, and if a station has many such tapes, it will want to obtain or make arrangements to use a BOSTIC high speed reader (300 CPS). However, it should be noted that there are no long waits for other stations to complete their turns before input can be started so that the 5 minutes it would take to input 3000 characters (or 25 feet of punched paper tape) may be preferable to walking to a station with more rapid input equipment. Also, it is possible to input a stream once and have it held for a number of runs without taking the time to re-input it--or to input a long stream and have it broken into sections with an identifier attached to each so that any subset of the whole can be selected for processing.



On the output side of the situation, whenever a large volume of output is required, it is desirable to have it printed on a line printer to avoid tying up the Teletype. This is particularly appropriate when small parts of the output are worthless or nearly worthless until all of it is available to the analyst. Four choices of disposition of results are available to RYE users. One may require that (1) output be forwarded to the requesting station only (regardless of the delay encountered before that station is on the air and free to receive--a valuable insurance for some compartmented problems); (2) one may request output to the station, if it is up, otherwise printer output; (3) output to the station, if it is not busy, otherwise printer; (4) printer output regardless, so that the station does not have to stay on the air after normal working hours or will not be tied up if a pressing problem comes along.

BOSTIC readers are able to accept paper tape at 300 characters per second and in either manual or automatic mode. They require an associated Teletype to initiate the request and receive back the receipt for the job. They can also be used for punching out long paper tape results (for example, weight tapes and crib banks which one wishes to keep on file for later input).

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The remote printers operate at 300 lines per minute. They normally have paper of the same size as the Teletypes (8 1/2 x 11) and can be used to provide faster output in the same format as the Teletypes. A computer printer is always available as an output device.

#### PROGRAMS AVAILABLE

In addition to many specially written programs for specific projects, several General Utility Programs (Guppies) which should be of use to analysts from various areas are available. These can be divided into several groups:

##### A. DIAGNOSTIC PROGRAMS

**BIG STET**--a large flexible stethoscope package which will accept up to about 100 messages and a total of 24,000 characters and which will allow the user to select the subprograms and options he wishes.

**DIANA**--allowing printout of digraphic identities and statistics on ten sets of digraphs where the wanted set is specified by I, J, and K parameters. I indicates the position of the first character of the first digraph of a set, J the increment to reach the second character of the same digraph, and K the increment to be added to I and J to locate the next digraph of the set.

**INDEX**--a flexible index for up to about 30,000 characters where the records to be sorted can be up to line length and cut from the stream in assorted ways; the control or sort key can consist of any 15 characters available in the record; the input alphabet can be specified by the user in any order he wishes as well as any coding which can be punched in 6 levels of paper tape; the output print format is also under his control.

**EPIC (Epictetus)**--program which saves more information about the location of roughness found in columns of a write-out of message beginnings and/or endings, or in groups formed by summing or differencing groups and columns from this write-out.

**FINKSBURG** will provide various level counts, etc., for 5-level paper tapes.

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~

B. MATCHING PROGRAMS

XIBAR permits a non-homogeneous batch of distributions to be broken down into sets so that the cross hitting between members of the set is as good or better than the average internal hitting of the whole batch of distributions.

CASANOVA

C. EDITING PROGRAMS

These programs perform a variety of editing functions on a single stream or a pair of streams and output results on command to the station or for input to another program. Functions which are provided include MASK (eliminates bits from a stream according to the unpunched positions of a mask tape), DOBE (1 for 1, 2 for 1, or 1 for 2 substitution), DROP-KEEP (drops or keeps specified codings), INDEED (inserts into or deletes from a stream according to a pattern), NEPTUNE (local transposition of elements within a given span of a stream), DELT (combines two streams by sum or difference of characters), LACER (interlaces a specified number of characters from one stream with a specified number from the other stream).

D. EXPLOITATION PROGRAMS

To make possible the exploitation of situations not readily handled by hand but easily managed by a computer.

GEEWHIZZER--locates stretches of cipher which combine with other stretches to produce plain-text digraphs to break into simple transposition cipher.

HUSK--

SCOOT--

(--Digested from the NSA Technical Journal, Vol IX, No. 2, May 1964)

~~TOP SECRET UMBRA~~

GUPPY MOTHER SWIMS WITH TIDE

by Peggy Barnhill, B42

Carolyn Palmer gets excited when she talks about RYE/TIDE and AUTOLINE, and well she might. She realizes how far the techniques and equipment have advanced in the past twenty-odd years, and her achievement in the field of computer cryptanalysis dates practically from the initial combination of the two terms. When Miss Palmer arrived at AFSA in 1951 with a freshly awarded M.A. in Math, the "computers" were limited to analog machines and EAM or RAM equipment.

One of Miss Palmer's initial assignments was with a group of cryptanalytic gurus who combined their talents to achieve a seldom heard-of success--they read a one-time pad system. With that achievement to inspire her, it is easy to understand how Carolyn became one of our most dedicated succeeders.

As part of what later became P1, she also spent some time evaluating the KW-26, a piece of U.S. cryptographic gear. While that equipment proved to be a little better than that of the competition, the correction of several flaws which were found made it much more reliable...so reliable, in fact, that it still constitutes a major portion of the U.S. cryptographics inventory.

Carolyn was introduced to programming when necessity called for training a nucleus of BOGART programmers. The ensuing course, which Miss Palmer describes as comparing favorably with survival training, produced some of the best programmers we have. Its graduates put together the BOGART version of STET, a grandfather of the present-day crypt diagnostic programs.

The BOGART STET was a great advance, but a problem developed because of the program's popularity. People were using STET to make 53 measurements of a cipher stream when they really wanted only three. To solve the problem, Carolyn began the development of the GUPPIES. These short, general-purpose cryptodiagnostics were installed on ROBROY and, with little variation as capability of the system advanced, they are much the same today. While she didn't write all of the GUPPY programs, Carolyn was generally responsible for them. She is therefore most widely known as the "GUPPY Mother."

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

*With the upgrade of the system that the installation of RYE brought, Carolyn began to see the concepts originally envisioned for ROBROY come into being. Not content with that success, she began planning for what has become the TIDE/AUTOLINE system today. Today she is planning the system of tomorrow. And considering the advance made so far, and being aware of her insight and what a co-worker describes as her "unreasonably good programming ability," we are sure that tomorrow's system will be as much of an advance over the TIDE of today as TIDE is over the ROBROY of yesterday.*

*We don't want to give the impression that Miss Palmer lives each day to "do or die for DIRNSA;" she has other interests. She possesses the love of good music which seems to be present in nearly all "computer-type" people and is a regular subscriber to the National Symphony. When her schedule permits, Carolyn spends time relaxing in the nearby Virginia mountains or visiting with a family whose members are scattered along the East Coast from New York to the Florida Keys.*



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~ONE CHANCE IN THREE---BUT IT WORKED

by William Gerhard, B6

ARDF needs no trumpeters in B Group, in ASA, or in AFSS. But important as the ARDF program was to become, experts in 1961 and early 1962 doubted that the first experiment involving direction finding and an L-20 aircraft would prove successful. As it turned out, there was one chance in three that the experiment which led to the ARDF program in Vietnam would, in fact, work at all. The following excerpts from an interview of Mr. H. S. Hovey, D/Ch of Staff for R&D, Hq, USASA, by Mr. L. L. Sternbeck and Mr. J. Gilbert of ASA shed some light on the first ARDF birds to fly for the U.S. in Vietnam; on the early improvising by ASA innovators; and, despite odds against them, on their success.

Why ARDF was Required in the First Place

*Q. Prior to ASA's becoming involved in ARDF development, was there any ongoing development of the capability within the Army?*

*A. The answer is really no. There had been, of course, a lot of development of ADF (airborne direction finding) systems for navigation purposes, which don't operate in the HF range and also the FM homers and other VHF navigation systems.*

*Q. ...The question I always had...Why was it so difficult for us to do that?*

*A. ...There is actually a technical explanation for why this difficulty occurs...the Vietnamese and the VC were using low power radios. Now, how do I get in HF a low powered radio... say, a one-watt power...to transmit a hundred miles? Well, the way to do that is to use a horizontal antenna, radiate the energy up to the ionosphere; then the ionosphere causes it to reflect down on the point you want. That means almost no energy is going out directly, so you sit over here on the ground with your direction finder even a half mile away, and there is no ground wave energy to hear. Now, an interceptor can listen because the sky wave is coming down from the ionosphere. I can sit there and copy what he is saying, but when I try to take a bearing, I am trying to take a bearing almost straight up, and there is just no way you are going to do that. Intercept is fine from steeply incident*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

skywaves, but DF needs a much more stable propagation path. The salvation is ARDF...you get a line of sight to him essentially, and there is now enough direct wave energy for you to operate with. You still must discriminate against the vertically incident energy. That was what had defied everybody because at these frequencies the aircraft dimensions are about the same as an antenna. So then all this steeply incident energy comes down on the airplane, and the skin of the aircraft is excited with RF currents. Your antenna is coupled into it and all you get is a hodgepodge...the one great thing we learned technically was how you could make a system that decouples from the plane, discriminates against the sky wave energy, and operates on the direct wave energy. Now on the broadcast band you don't have that problem. You are talking large power and a lot of energy that is vertically polarized [and] radiated out. The same with VHF. The VHF will not come back down from the ionosphere. That is exactly why the Viet Cong used this [HF] frequency, because it did support propagation...

It was October/November of 1961 when the urgent requirement came out of Vietnam because they [3rd RRU members] had gone in-country and were trying to use AN/PRD-1s, and they couldn't. The AN/PRD-1 is a ground loop type DF set and needs a good ground wave signal to work against. A cable came back asking us what we suggested or what we could do.

#### The Experiment

*Q. Was this the 3rd RRU?*

A. Our 3rd RRU and specifically...WO George Miller. I was the project officer for direction finding systems in these days. George Miller and I---I had the action here through command channels and he had the action there---had this exchange of messages; there were probably 10 or 12 messages in that sequence. We worried about how to improve the AN/TRD-4s, which is the larger DF set and what we were going to do with his AN/PRD-1s. Then we got on to what we could do to solve it. That was where the idea of trying the aircraft emerged. We thought an aircraft would be useful, and he agreed that probably the aircraft would be great. In November, about Thanksgiving, I went over to Vietnam along with an engineer named Harold Jaffe from ECOM [U.S. Army Electronics Command].....So we went over and spent a month in Vietnam and wandered around with George Miller and the rest of the people involved. We went around on PRD-1 operations ourselves, took receivers and listened, making measurements of what the propagation conditions were.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Q. When and under what circumstances did ASA first become involved with research [and] development of ARDF? Was it a result of the 3rd RRU's recommendation? MACV's? Department of the Army's?

A. You can summarize it by saying that the way we got involved was reacting to the problem--that they couldn't use AN/PRD-1s to do the job and the proposition was "could we use airplanes?" And the answer was "Yes, we think we can."

Q. You got together with ECOM on this and went out with Mr. Jaffe?

A. Exactly.

Q. When did you bring Department of the Army into this?

A. We didn't really...this whole thing was done on a shoe-string. There were no external contracts made during this time frame; all was done in-house at ECOM. There were very few approvals obtained because we weren't talking dollar levels that required any approvals. Secondly, there wasn't a great deal of attention that was attracted in this time frame in the eyes of the Department of the Army. The 3rd RRU was calling for a solution, but it was to ASA. So it was later on that major involvement on the part of DA took place...

Q. Were the pilots organic to the unit [3rd RRU]?

A. Yes. I don't know how they came to be, but LTC Cochrane [CO, 3rd RRU, Saigon] had acquired two pilots, one a CPT Bill Simpson, who later came and worked here, and CPT Don Schessler. They were both Transportation Corps officers and didn't know anything about ASA until they came in. I believe a lot of credit belongs to them for having operated the thing.

Q. Did they come explicitly for this project?

A. Yes, that was something the 3rd RRU had arranged. We went out the first time feeling we could produce the gadget, and LTC Cochrane handled the arrangements for getting aircraft which he borrowed from a Signal Unit, I believe, and the two pilots. Later we came back with the equipment and put it on.

Q. The first planes flew in March of 1962?

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

A. Right.

Q. How much testing were you doing there?

A. We were running a pretty extensive program. In the first place, it was a fairly simple system, although it performed an elegant solution. We had done work earlier with VHF ground direction finder, a thing called AN/TRD-16, which ECOM developed, which is composed of a pair of antennas differentially connected. That was a very effective ground direction finder in the VHF. That was the technology which we applied to the HF but increased the spacing between antennas. In terms of hardware you weren't talking a great deal--a receiver, some cables, the antennas on the aircraft, and a little bit of circuitry to connect them. That was the size of it in the first version. It was a kind of thing which did not require weeks and weeks of fabrication. It did require an awful lot of testing. A whole series of antennas were tried to get out of the coupling problem with the airframe--that was going on at Fort Monmouth--the actual testing. When we felt we had something, we were able just to use the shops at Monmouth to fabricate antennas, cables, and other things and rush over and install them ourselves....

Q. Was there any training involved by the pilots and operators?

A. There was a lot of training by the pilot. This was very demanding of the pilot because he had no navigation system which would tell him where the airplane was at the time he was taking the bearing. He had to learn to fly over a point on the ground that he could then identify on his map as he took a bearing. The operator who was flying with him with a map had the duty of operating the receiver. The operator's task was not too different from the one he had operating the PRD-1 or an intercept position. He had to find the signal frequency and copy it, making sure he was on the right one. So that was pretty much what he was used to on the ground except he now was in a plane and had all the risks of getting air sick, etc. But really the pilot was the one who had to do this by pointing the aircraft at the target and slueing the tail back and forth, reading on his gyrocompass while he was still over ground he could recognize. A skilled pilot can do that very well, but this is something the average Army aviator isn't trained to do.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

When we installed the thing, we worked a couple of days with the pilots there, refining it. We flew a lot of hours ourselves. They caught on very quickly. To prove what we had done, we had a hidden transmitter hunt. The 3rd RRU hid some transmitters around Saigon and they went out and found them.

If the pilot was careful in finding a bearing, even this first system could be incredibly accurate. For instance, during this hidden transmitter test the system showed which side of a road at a junction the transmitters were. We were talking even then about accuracies of hundreds of meters.

*Q. Why were the L-20 aircraft selected for ARDF? Where in the United States, and when, did the initial ARDF testing take place?*

*A. ....We found out that this aircraft was fairly available over there. It was adequate for our purposes because you needed something with good visibility; it could carry two or three people and some equipment....The L-20 just happened to be a very nice airplane for the purpose. The big thing was, it was available over here and could be maintained because the MACV Flight Detachment was who their people worked with in the beginning--the old MAAG [Military Assistance Advisory Group] Flight Detachment, actually. The Detachment had L-20s.*

*Q. Was it the Signal Corps from whom we had borrowed the early planes?*

*A. Yes, it was the Signal Corps we got the aircraft from.*

We had the one aircraft at Monmouth from the Flight Detachment that we had put the antennas on and it eventually worked out very well. That became the basis of the system we took over. We went over with equipment to do three airplanes. As I say, this went as luggage. I went; Harold Jaffe, the ECOM project engineer, went; a technician from ECOM by the name of Walter Day went; and an airplane technician by the name of Danny Shargus. Danny's job was to mount the antennas on the aircraft. Walter Day was the electronic technician who was to help Jaffe and me get the system together. Jaffe and I did most of the flying.

So we had this airplane which worked well at Monmouth. We went to Vietnam, and they had arranged three airplanes to work with. The first plane we put it on, it worked very well. This

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

is the one we did the hidden transmitter hunt from. As soon as that day was over, they took it away from us. We wanted to test a little more, but they figured it worked well enough so that it went into operation. We did fly some operational missions with them for a while to make sure things were working. We worked on the other two L-20s, but neither one of those aircraft worked. We installed the systems and sweated blood for several weeks and finally just had to plain give up. We couldn't make the systems work on these two planes. The reason for it had to do with the way the aircraft themselves are constructed. We apparently had some type of unsymmetrical airframe current distribution. As long as that is symmetrical and you can maintain a decoupling from it, your system will work. But some of the L-20s had been through extensive rehab. The inboard ends of the wings had been painted more coats on the one than the other, and things like this. When they had been put back together you had a terribly unsymmetrical RF current distribution, and we had no way to adjust for that at the time.

At that time, we found ourselves literally faced with the problem of selecting airplanes. We wound up then leaving those two which worked quite poorly and one which worked very well. Aircraft tail #5682 was the good one and #33731 and 37963 were the poor ones. We came home and chose airplanes. ECOM sent people--Walt Day, I believe, from airfield to airfield finding planes which had not been through this major rehab, equipped two, tested them here, loaded them on board an aircraft, and flew them out to Vietnam to give the 3rd RRU the three it was after. The planes they had which didn't work well went back to where they came from. The 3rd RRU wound up then with three working L-20s after that ordeal. Actually, the ECOM lab A/C #55151 and #82012 were the ones that were sent out.

Now, I said there was divine intervention. It turned out historically that one out of the three aircraft worked successfully with this system on it. So the odds were very much in favor that we would have gotten a bad plane in the beginning at Monmouth or that we should have gotten a bad plane in the beginning in Vietnam. Given the suspicion (or skepticism) about ARDF--we could have very well stopped, had that happened--and here very competent people had said it couldn't be done anyway. There may not have been such a thing as ARDF today. It was a fortuitous thing and something we speculated about.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Q. Do you have any...anecdotes related to the development of ARDF...?

A. I think this business of taking it out as luggage. And the pilots would have been far more worried than they were if they had known just who mounted some of these systems, because all of us wound up riveting things on airplanes. I did. We almost lost it all in Hawaii when they misrouted all our luggage. We had to go at the last minute and dig that out of another Pan American aircraft. I think the selection of aircraft is also significant.

One of the things we took some technical satisfaction in was a little event out there when we were flying the first one. What we would do was to fly to Bien Hoa where we had a DF site and the flash transmitter which controlled our DF nets in Saigon. So we would fly over our DF site at Bien Hoa and shoot that flash transmitter, taking a bearing on it because that was one of the check bearings they used that was supposedly quite accurate. We worked a couple of days because there were a couple of degrees error, and finally in disgust went back and recomputed the check bearing and found out it had been calculated wrong and that the aircraft had been correct all this time.

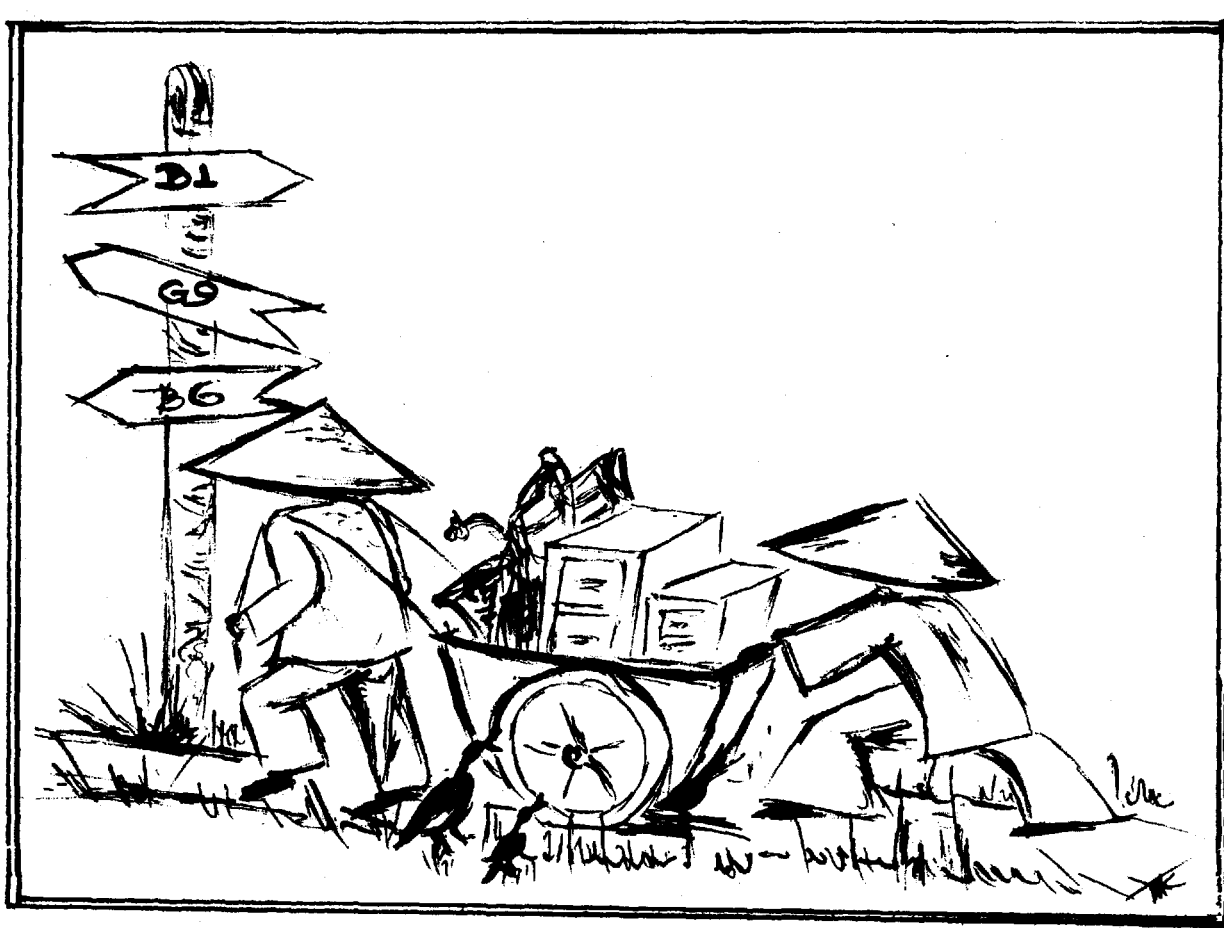
\*\*\*\*

*"The Wise Man, when abroad,  
Impartial to the world,  
Does not divide or judge.  
But people everywhere  
Mark well his ears and eyes;  
For wise men hear and see  
As little children do."*

---Lao Tzu

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



"The gem cannot be polished without friction,  
nor man perfected without trials."

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

MARKETING OUR PRODUCT

by Walter D. Abbott, Jr., B6

Many of us involved in the production elements of this Agency have heard the expression, "Product is our only product." The capabilities, successes, and even the shortcomings of our intelligence apparatus are amply documented by the myriad of products released by this Agency on a daily basis, and overall, speak quite eloquently for the talents, dedication, and technical skills of the people devoted to intelligence production within NSA.

Recognizing that we are dealing with a fluid cast of product recipients (many of whom may only recently have become involved in the intelligence business), and recognizing that some of our subjects and jargon might be considered technical, confusing, or perhaps even mystifying to the casual reader, we have set up a system of user service centers, known variously as Cryptologic Support Group (CSG), NSA Operations Group (NOG), and Intelligence Support Staff (ISS), to assist the user in understanding and interpreting the product he receives. These organizations have often demonstrated their functional utility and have periodically reflected quite favorably on NSA. The quality of these operations has not, however, been consistently excellent, and this is the point I intend to address.

The success of any product service operation is contingent on the people manning the operation. Most of our operations located at major command headquarters outside the Washington area are manned primarily by NSA civilians whose function is to advise and support their military counterparts. For many military personnel, the people they meet at the product service organization will be the only NSA people they will be exposed to during their military career, and the impressions they form of the Agency itself will be influenced by the impressions they have of the NSA people they have met. It is therefore extremely important to give these command personnel the most positive, favorable, impression we can.

We ostensibly endeavor to ensure that this happens. We select personnel for the product service organizations who are generally very knowledgeable on some target entity, have a demonstrated talent or skill, and are considered "experts" or "near experts" in their field. This is, however, only one part of the

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

selection process. We also select people who need a job change for professional or career development reasons; people who are the only candidates for a particular position (at which time skill, talent, etc., become secondary); or people who have either never been overseas or have not been overseas in many years. In recent months a prevalent opinion is that this latter criterion is an overriding factor in overseas selection.

We normally do not select people because they have performed such jobs in the past and demonstrated real skill at handling such jobs. We do not have, for instance, a cadre of overseas specialists who not only are SIGINT specialists, but also are versed in command structure and relationships and capable of doing a good job in a command environment. Rather, we endeavor to "spread the wealth" and by so doing, we sometimes end up a bit poorer than when we started.

I am not condemning the system as it exists. I am merely offering suggestions which I feel might improve it and give the Agency a better image overseas.

First, I strongly advocate that at least some selections be based on past performance in the field. If a person has demonstrated an ability to represent NSA with excellence, he should be allowed to serve again as soon as possible or to continue to serve if he is already on the job. I know and know of several individuals who have done truly outstanding jobs overseas, who were functioning well, were happy where they were, and wanted to stay but had to come back to NSA because their tours were up. They had little or no prospect of returning to the overseas area. Excluding the cost considerations (the expense involved in rotating families is not insignificant), the Agency opted to replace a known commodity (i.e., a man who was a good Agency representative) with an unknown (or at least untested) commodity for reasons which to me are less than clear. I suggest the system needs to examine its inflexibility and consider each man on a case-by-case basis. The result should be beneficial to the Agency, and that seems to me to be the paramount issue.

My second recommendation is that all NSA personnel, before they are sent to an overseas job which demands continuing exposure to non-NSA personnel, be given a series of training courses dealing with personal interaction, as well as command relationships and responsibilities. Too often our people forget

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

that the person in the command intelligence shop is frequently new to the business and may have been a weapons system operator for ten years before being given a Special Intelligence clearance. Questions from that individual might seem stupid, trivial or a waste of time to the NSA person who has been involved in the cryptologic business most of his adult life, but he should attempt to answer them without condescension. Moreover, the NSA people should get to know their counterparts and be able to relate to them, on and off the job. Superior, aloof, indifferent, and arrogant attitudes have no place in our overseas operations. But they exist and they hurt us. We should expend all necessary efforts to develop a sense of trust and confidence in the people we support. If that can be achieved, the entire support operation of the Agency will benefit.

The training program should include a little "Madison Avenue" public relations training and a brief exposure to salesmanship. It is not enough to be a good analyst, technician or reporter. The individual also must be a good representative of this Agency, able to convince his command counterparts that our product is worth their attention, and that we honestly want to satisfy the command requirements, regardless of our individual propensities. We have a very saleable product. We need to develop the personnel to promote our product. It might be worth the investment for the Agency to explore various industrial programs geared to developing a sales force. The "foot-in-the-door" syndrome has applicability in our business, and developing a training program to foster this is, in my opinion, both worthwhile and necessary.

Again let me state that I am not faulting the existing system so much as offering ways in which it might be improved. We have a good product and a ready market for it. Let's market it properly, and make friends for the Agency in the process. Let's do it right.

~~TOP SECRET UMBRA~~

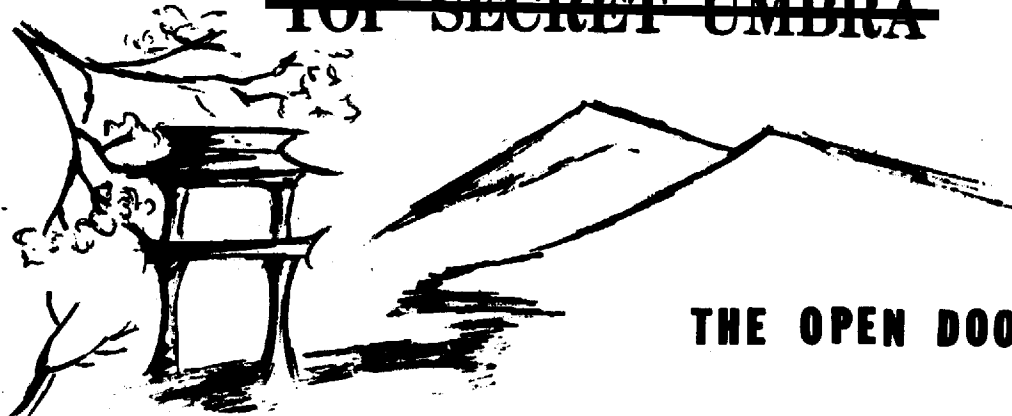


~~TOP SECRET UMBRA~~

Transposition is...

This month's puzzle has pairs of twists. Can you solve it?

GERTM	CUSEL	AEPIM	SFTON	SEIEA
UNDMI	HUDRF	YHORI	EHONL	IEPAU
VEEEU	NFMFO	EWTYW	ONTNO	OTRIX
AEELE	NMGEF	UKOII	HTETE	DHNGI
ITAWM	KEARE	EHNRS	EVSAR	ETRAF
TSINA	ELLYN	HAEDX	MORID	YRUXN
OETII	NNSXS	LGFNT	OEISS	HDDWN
SALFT	PXIUI	VIUER	OAMED	HNENA
XRRAT	EIIWC	DNTRD	AUOIK	DSAER
ORHEH	AOTTP	GNEEG	LTRME	SNNFO
SITSH	ETAOA	SPLYO	EUSHM	DEXNS
SCELN	RAAAE	DPLYI	UOEON	EATEC
HIOET	RNSOX	ITBAT	OLRDM	OHOSA
DOCSX	SOOSE	IONSL	UOSTD	HLDTA
EXASV	ENSBS	UPADI	EDYEN	TCEAE
TTMHV	HRRXR	CDTER	THCNX	EFPLA
DHGOH	GTTOD	TEBCO	RMTUO	DMRMP
ATUAD	NIDWI	FRI RT	ICIOH	SEEEI
AXTET	HWORE	ATIVL	LELIE	SFEAI
YHCSF	ILIFX	EPTRN	MSOXR	DPLEA
SEDRT	HYEOT	SLWIM	RMCBN	OIGSP
TWLOO	IEIRF	TNFAD	OORSN	MEHTS
OTLFI	SPNWA	CGBEI	LTCTI	ESABH
OMMAD	UFONL	EHAHM	STFNI	IHOEI
GNMOO	OIFGO	EPOAG	WBDCC	LAAXS
SYTNH	GSNAS	OOTDN	SLXNA	DDASE
ISNHI	ISTLT	HCOOE	RSAHT	EMNOV
AALCA	ZUKAO	TAMET	CSNEU	LEENR
TCTDN	UNOAR	FLHRI	GFDLC	RANMT
ONAH T	ISHER	OMEES	DKSHN	IILOW
SREEE	YRITL	OOUSX	FCEDI	TEOXI
NESEH	OEINN	TSNTN	SYDYD	SENTN
GSNEE	ODEOT	ATENN	H	

~~TOP SECRET UMBRA~~**THE OPEN DOOR**

*We seek to be companions along the way.  
 The lantern which we carry is not ours.  
 The spirit which we share is contagious thought;  
 The knowledge which we gain, an illuminating torch  
 And all who seek may perceive and learn.*

*-The Concept of Dragon Seeds*

THE "C" PARALLELOGRAM, OR A VIETNAM COVER STORY

by Bee Kennard, P222

"Lessons Learned in Vietnam" was the title of an army publication describing the latest combat developments in the ground war. SIGINT learned many lessons there as well; but for the most part, the participants have been too busy fighting to bother with writing about their experiences. The Vietnam war was also an education for the information analyst providing battlefield support. While the lesson is still fresh and the topic timely, this particular contribution to the war effort is believed worth sharing and passing on.

The Monsoons Came

Times have changed since Napoleon, for a modern army travels on paper. It simply cannot function without a piece of paper telling it where to go and what to do and how to do it. The Viet Cong/North Vietnamese Army had paper, paper everywhere. Torrents of infiltration passes, invoices, manifests, supply lists poured down the Ho Chi Minh trail. Files, records, accounts, inventories, manuals, directives flooded the base camps. Marching orders, firing tables, target studies, attack plans swamped the battlefields. And floating on top of the official paper sea were the personal diaries kept by every VC soldier from private to general. If the info analyst could survive the inundation, captured enemy documents made Vietnam an intelligence paradise.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The Communist proclivity for secrecy compounded the red tape because everything and everybody had a cover name which changed constantly. A drifting cover designator list became a lifeline for the drowning analyst to latch onto. Studying for dear life, the cover designator lists revealed an identification system that was intricate, minute, and precise. There were two main channels, military and party, and each had a four-part cover address consisting of a cover name, a cover number, the official letter box number, and the personal letter box number. Every military unit from division to company had the four-part code which was different at each echelon. The party organization and its agencies at the district, province, and regional level were assigned a multi-part cover address. There were separate sets of cover designators for intra- and inter-regional correspondence and between North and South Vietnam. The party used family relationships to denote echelon while the military used the government administrative structure. Leaders favored numbers for cover names. The VC cover system was controlled from the top and carefully regulated. Once the patterns were mastered, the info analyst could knife through the complicated tide with ease and dispatch.

#### Communications Problems

Buoyed with success and armed with the trustworthy VC cover system, the info analyst turns next to bail out the SIGINT analyst. However, SIGINT has its own identification system for VC targets, and in another language yet: radio station designators, case notations, crypt systems, callsigns. The two systems would not mesh. Not only do SIGINT and collateral not speak the same language, but also there is unreasonable doubt that the two are even in the same ball park. What can you do with a can of worms that wiggle off in all directions? Common sense to the rescue. The first step was to set up two columns, SIGINT and collateral, and jot down just the bare facts under either heading. This move put a stop to the confusion over nomenclature. Lined up side by side, the next step was to match the VC cover with its SIGINT counterpart. Some pairs were easy to hitch together, but others balked and got downright obstinate. So we applied psychology. Any analyst handling voluminous material over a lengthy period develops a feel for his subject, but these feelings are seldom expressed or written down. This intuitive knowledge spells the difference between success and failure. Altogether, the parallel format, the fusion technique, and the inductive approach proved a sensible, workable arrangement. A number of secret VC targets were identified.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~Parallel Construction

Here is a shining example of what this device can do with a really tough problem. The story uncovered by your war correspondent has everything: action, suspense, mystery, intrigue, a devious plot with a surprise ending, and a search that ranges from steaming jungles to elegant drawing rooms and races to a thrilling climax at zero hour in a mountain hideaway. Since the facts do not always speak for themselves, interpretive comments have been included to aid the uninitiated. Lights, camera, ACTION!

CollateralSIGINT

C mentioned briefly in directive on expansion and development of crypto branches, Region 1.

C from content apparently crypto agency on higher level than COSVN (Central Office for South Vietnam), the VC head organization.

Date of info: 3 Jan 66

Source: captured document

Comment: An unobtrusive beginning.

C both sent and received messages.

C messages more strategic than those addressed to R (cover designator for COSVN).

C cadre operated command post in (VC) Military Region 3.

C radio operators and crypto personnel infiltrated to MR3 in Aug 1970.

C radio equipment dispatched to MR3 Oct 70.

Date of info: 1969-70

Source: captured message register, code books of Signal/Crypto Branches, MR3

Comment: ARVN J2 study dtd 11 Mar 71 established that:

- C does exist.
- C is different from and higher echelon than COSVN.
- C has operated in delta region of SVN since at least 1968.

Comment: Communications links between MR3 Hq and High Command were the same as those with other known military regions. Until Oct 71, MR3 Hq continued to use a signals plan involving call-signs from a system which was

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~Collateral

Conclusion: ARVN J2 opined that Agency C is the Forward Command Post of NVA High Command, Hanoi.

SIGINT

generally replaced in late 65/early 66. An unusual feature which could not be explained.

Col Nguyen Van Sau to return immediately from Front 4 (in Danang area) for urgent work with General Staff in Hanoi. Car transportation arranged.

Date of info: Apr 71

Source: Intercepted message of 559 Transportation Group.

Comment: To spell out the full name in traffic is never--well, hardly ever--done. This rare occurrence constituted a real breach of security. The colonel must really be important to rate a private automobile in transport-scarce North Vietnam. Could he be the same man found in collateral?

Nguyen Van Sau signed leave authorization for command of CP.40, Central Executive Committee, Lao Dong Party.

Date of info: 17 May 65

Source: captured document

Comment: An innocuous tidbit--but follow where it leads.

CP.40

Commander: Lt Gen Nguyen Van Vinh

Location: Hanoi, 96 Quoc Tu Giam Street

Mission: Secret military command center directing Liberation Front activities in SVN.

Organization: Diplomatic Office  
Planning Office  
Civilian/Military Affairs  
Finance/Economy Office

Date of info: late 1966

Source: VC POW

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~CollateralSIGINT

Comment: The plot thickens. Isn't it incongruous for a military outfit to engage in diplomacy? Or is CP.40 strictly military? What business does the finance office transact?

Central Reunification Committee

Chief: Lt Gen Nguyen Van Vinh  
(See above for connection.)

Mission: Executive agency of Politburo. Directs and coordinates all military and political activities in SVN. COSVN is responsible to CEC thru CRC. Staff Hq for conduct of Liberation War in SVN. No communications of its own. Ministry of Defense provides all communications facilities.

Date of info: June 67

Source: VC rallier

Comment: If the CRC uses the military communications system for the military side of its mission, then it could use party and dip comms for its political and diplomatic functions. The scene shifts.

3 Jan 69, new routing designator on traffic from Special Delegation in Paris. Msg relayed to COSVN by CEC, Hanoi. Feb 69, new routing designators on Paris messages for both Hanoi and COSVN. Then two more groups appeared: Phnom Penh-Hanoi-Peiching, and COSVN-Hanoi-Phnom Penh.

Any msg originated by one intended for other two.

Phnom Penh link last observed Apr 70 following break in dip relations.

Hanoi and Paris messages predominate. From SIGINT viewpoint, the new designation system on dip-party comms is unique because:

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~CollateralSIGINT

1. Routing designators in addition to and different from dip mission designators.

2. Msg technical characteristics similar to but unlike dip post comms.

3. Msg between foreign NVN embassies is infrequent.

4. COSVN involvement with NVN dip posts for first time.

Source: 2/00/VCD/R14-72 dtd 17 Oct 72

Comment: To sum up, we have an organization which used the dip crypt system and the dip communications network but is not part of the dip establishment. What organization fits this description? The Central Reunification Committee. The CRC has a man in Paris and with COSVN and had a man in Phnom Penh and Peiching. CEC, Hanoi, which relays the Paris messages, is the diplomatic office of the CRC and the triple axes were the CRC dip communications net. An exciting development! We're off in hot pursuit.

Footnote: For what it's worth, the defunct PP-Hanoi-Peiching axis is believed the Finance Office of the CRC. It costs a lot of money to wage war. When the mob sacked the NVN Embassy, they really came out of the woodwork. Cambodia was the principal supplier for the Liberation Army, and Chinese aid to the VC was funneled through Cambodian ports. Doan 17 was the VC covername of a secret rear service group located in Phnom Penh. Its supply operations and finaglings in the international money marts

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~CollateralSIGINT

was a tightly held secret. When the Cambodian source was cut off, the VC became so desperate that maritime infiltration from NVN was again attempted. Remember those trawlers?

Map, showing observation points on Bach Ma and Ba Na mountains northwest and southwest of DaNang.

Date of info: Dec 68

Source: French newspaperman from Vietnamese delegation sources.

Comment: Just a nondescript map; but why that particular area of South Vietnam? What is the French connection with Region 5? Here was the key to the mystery in the answer to those two questions.

On 6 Mar 70 four new routing designators appeared on Paris-originated correspondence and were subsequently relayed by CEC, Hanoi to Region 5 Committee and Tri-Thien-Hue Committee. These Paris messages are usually passed one or two days after the Thursday meetings. The correspondence was not re-encrypted in a party system, but remained in the VC dip system.

Comment: A communications anomaly. Why should two subordinates of COSVN receive info copies? Or are the Paris msgs intended for a special office located in Region 5?

Cover designators for high level agencies:

Ca (elder brother) Dai-Central Party Hq  
 Cau (uncle) Ca-Central Reunification Committee  
 Cau (uncle) Vu-Central Military Affairs Party Committee

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~CollateralSIGINTAddress of C Command Committee:

c/o Gai Lai Provincial Unit,  
Darlac Provincial Unit, MR5

Date of info: about Mar 67

Source: Master list of CD-LBN designators for MR5 and MR6 classified (VC) Top Secret. Captured from postal battalion.

Comment: A prize document worth its weight in solid gold. It is the only CD list which gives the covernames of Lao Dong Party agencies. In our parlance, the document would bear the caveat HANDLE VIA COMINT CHANNELS ONLY because in VC practice only communications personnel had access to master CD lists. Agency C has a command post in MR5 as well as MR3. Is Agency C in both regions the Central Reunification Committee?

"Cau Ca" personnel roster. No. 2 man is political officer of "C." Nine regroupees assigned to 5 provinces in MR5.

All hard-core Communist cadre admitted to the party between 46-50.

Date of info: 18 Sep 67 or 68

Source: captured document

Comment: The clincher linking C to Cau Ca and the answer to the French connection with Region 5.

Premise: There exists in South Vietnam a deeply hidden top level decision group directing military operations.

Basis: Inadvertent disclosure by NVN delegation in Laos.

Date of info: July 62

Source: The definitive study "Viet Cong," by Douglas Pike.

Conclusion: C aka<sup>1</sup> Cau Ca aka CP.40 aka Central Reunification Committee is the hidden group which

<sup>1</sup>"also known as"

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Collateral

SIGINT

has been running the war all these years.

Comment: EUREKA! We finally blew their cover. The very name reunification is its own proof. No wonder the CRC went to such elaborate lengths to hide its name all these years--and successfully, too. The revelation does not materially change the tactical outcome of the war, but it certainly alters the entire strategic concept. Although the discovery came too late to help win the war, the knowledge may help to secure the peace. Following the signing of the ceasefire agreement, Le Duc Tho remarked that "reunification" is the postwar goal of North Vietnam. President Nixon hopes to persuade Hanoi to achieve the goal through political means.

REUNIFICATION is still the name of the game.

Epilogue: The Central Reunification Committee could not be isolated in SIGINT because it had no communications system of its own. Since the military, party, and diplomatic systems employed by the CRD were unreadable, the CRC could conceal its identity but not its existence. The oddity here, the anomaly there, the unique and different in communications behavior, attested to something passing strange. SIGINT could tell what it was not, but collateral told what it was. It takes both negative and positive evidence to prove the truth. Proving the negative is a grubby, thankless task and SIGINT had the harder part. Neither SIGINT nor collateral alone could have identified the Central Reunification Committee, but together they found it.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

After Action Report

Now is the time for a performance appraisal of the "parallelogram," focusing on how and why it works. First, note the striking format and how it clearly delineates the problem, throwing the known facts and gaps in sharp relief. The simple act of placing the facts side by side causes the sparks to fly upward. The parallel arrangement is all important for generating analysis and research. The analyst can tell at a glance what is missing and get straight to the point. Research will be a coordinated and directed effort instead of a hit or miss operation. With the whole picture before him, the individual analyst can see where his contribution fits and can better appreciate the group endeavor. To know your work has meaning and value in the compartmented world of intelligence gives a big lift to morale. Also, the parallel format provides an incentive for the individual analyst. Who can resist adding his piece to the puzzle?

Next, notice how SIGINT and collateral meet, understand, and reinforce each other. There has been limited fusion of SIGINT and collateral, but essentially each sticks to its own narrow track. No hits, no runs, no errors and no ball game. The info analyst who sees both the collateral and SIGINT viewpoints from the Agency's vantage point can build the bridge of understanding and get the two sides together to play ball. The fusion of the two viewpoints enlarges the vision, doubles the knowledge and resources of each side, and benefits the intelligence community as well. Fusion would soon remedy the execrable writing which afflicts SIGINT reporting. Why should the reader be forced to interpret what you mean standing on his head? If you can name the target instead of referring to it as an "unidentified high level authority," your sentence automatically becomes taut, crisp, and clear. Good riddance to bad weasel English would enhance our product and relieve our long suffering customers.

Finally, study how the inductive approach resolved the dilemma and untied the knot. As long as you are adding two plus two from either column, deduction can easily arrive at four. When you are dealing with unknowns (which is the usual equation in intelligence), you have to put the cart before the horse. However, the French inductive leap proceeds from Sherlock Holmes plodding. Just suppose the answer is five and eh, voila! see how she runs. Once you try looking in a new place the leads

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

will turn up and things start to click. Suddenly the light flashes on. You see the whole brilliant picture, you hear events falling into place, and you feel how every detail fits. It's a brand new ball game! To play in the big leagues requires a free style in analytical research. To succeed, you have to try harder but you will never know until you try. What have we got to lose but our ignorance?

#### Wave of the Future

The "parallelogram" has been tested on the battlefield and proved a practical and valuable tool. It is not a shortcut to success nor a substitute for work nor a formula to replace thinking. Indeed, analysts on both sides will have to hump to meet the high standards. No longer can either side go it alone or afford the luxury. The "parallelogram" is a sophisticated tool designed for qualitative analysis and research. With such specifications it is tailor-made for subtle, complex intelligence operations demanding integrated research in uncharted fields. Pioneering is for the brave, the bold, and the imaginative. Soaring on gossamer wings of faith and courage with the beacon of hope lighting the way, together we can meet the challenges of a future bright with promise. We recommend the parallelogram as the wave of the future. It's simple, it's beautiful, and it comes with a money-back guarantee.

*EDITOR'S NOTE: The above article has provoked comment among the editors and staff--not all favorable. We present it to you substantially as it was written in the interest of our "Open Door" policy. But we, and the author, would sincerely appreciate your comments on the article, the intelligence "fact" discussed, and the "new technique" represented by the parallelogram presentation.*

~~TOP SECRET UMBRA~~

# ~~TOP SECRET UMBRA~~

## CRYPTO-SCRAMBLE

By Richard Atkinson

Unscramble each of the five numbered crypto-scrambles, placing one letter in each space, to form five words or names, each of which fits the definition to its right.

1. L A T I C E D  
\_ \_ \_ \_ \_ O \_ \_ \_

Measure of 2's roughness.

2. P H O N O G R A M  
O O \_ \_ \_ \_ \_

See 1.

3. I C R A V E A G E  
O \_ \_ O \_ \_ \_ \_

Width test on STET.

4. M A G G I E S  
\_ \_ \_ O \_ \_ \_

Measure of deviation from normal.

5. B L E A T S  
\_ \_ \_ O \_ \_ \_

Rye program which generates tailor-made mathematical tables to YOUR specifications.

Now arrange the circled letters to form the cryptoanswer suggested by the cartoon at the right.

Print CRYPTOANSWER here.

\_\_\_\_\_

Answers on page 58



ONE WAY TO GET A RAG MAN.

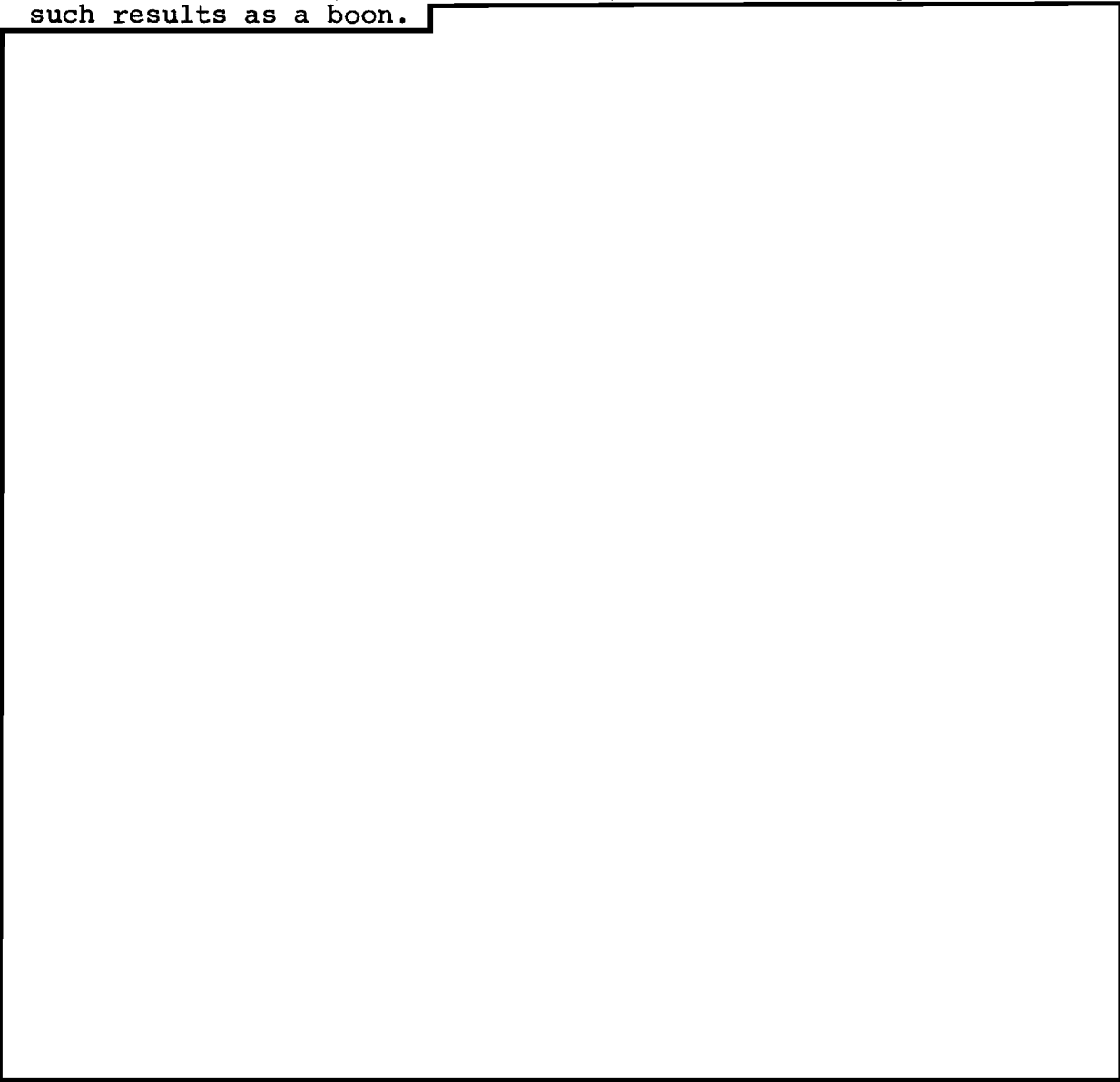
~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

REFLECTIONS ON A NON-RANDOM BANE

by Rodney Forbes, B43

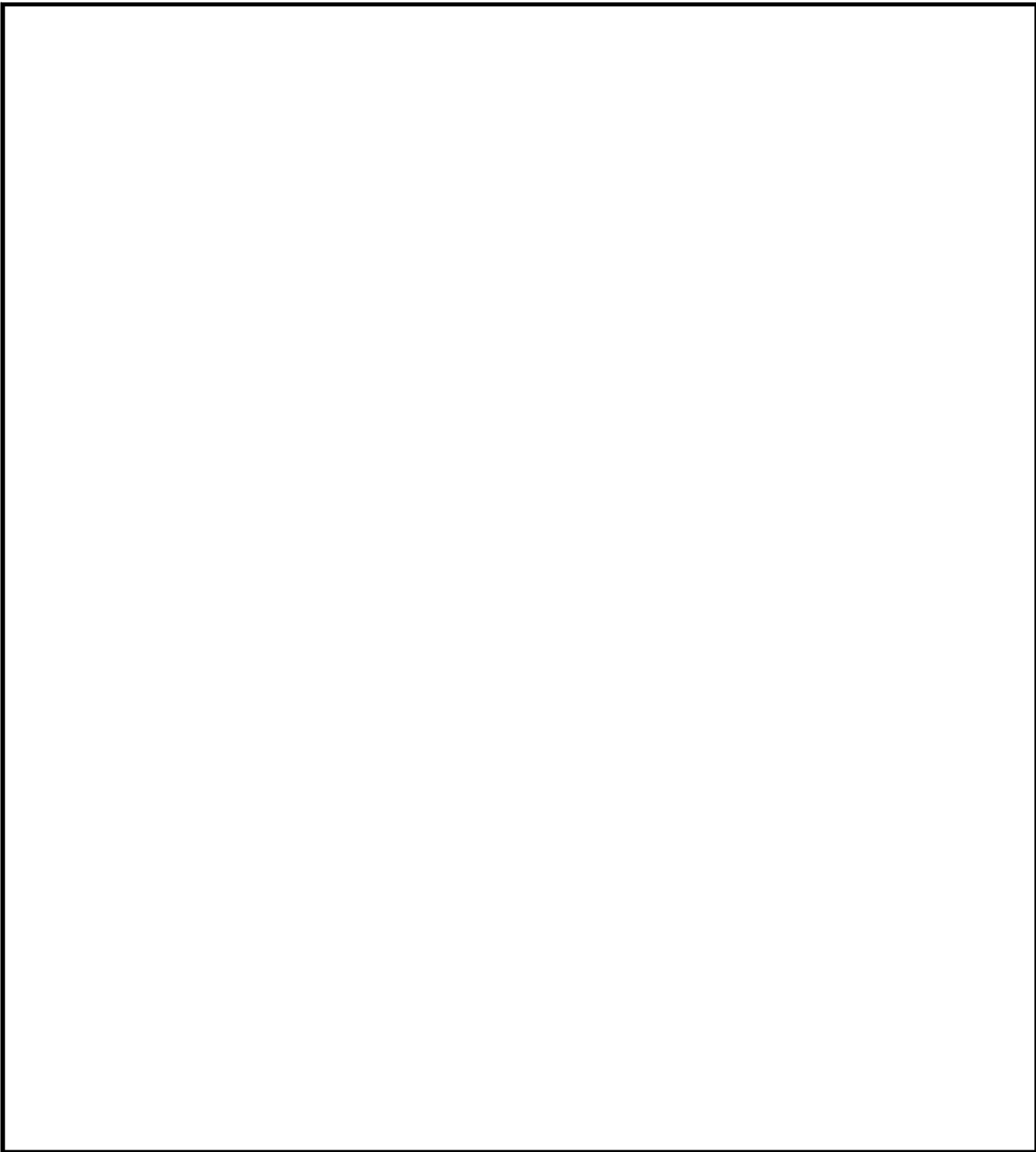
The cryptanalyst usually keeps his eyes open and his computers searching for non-random phenomena, and regards such results as a boon.



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

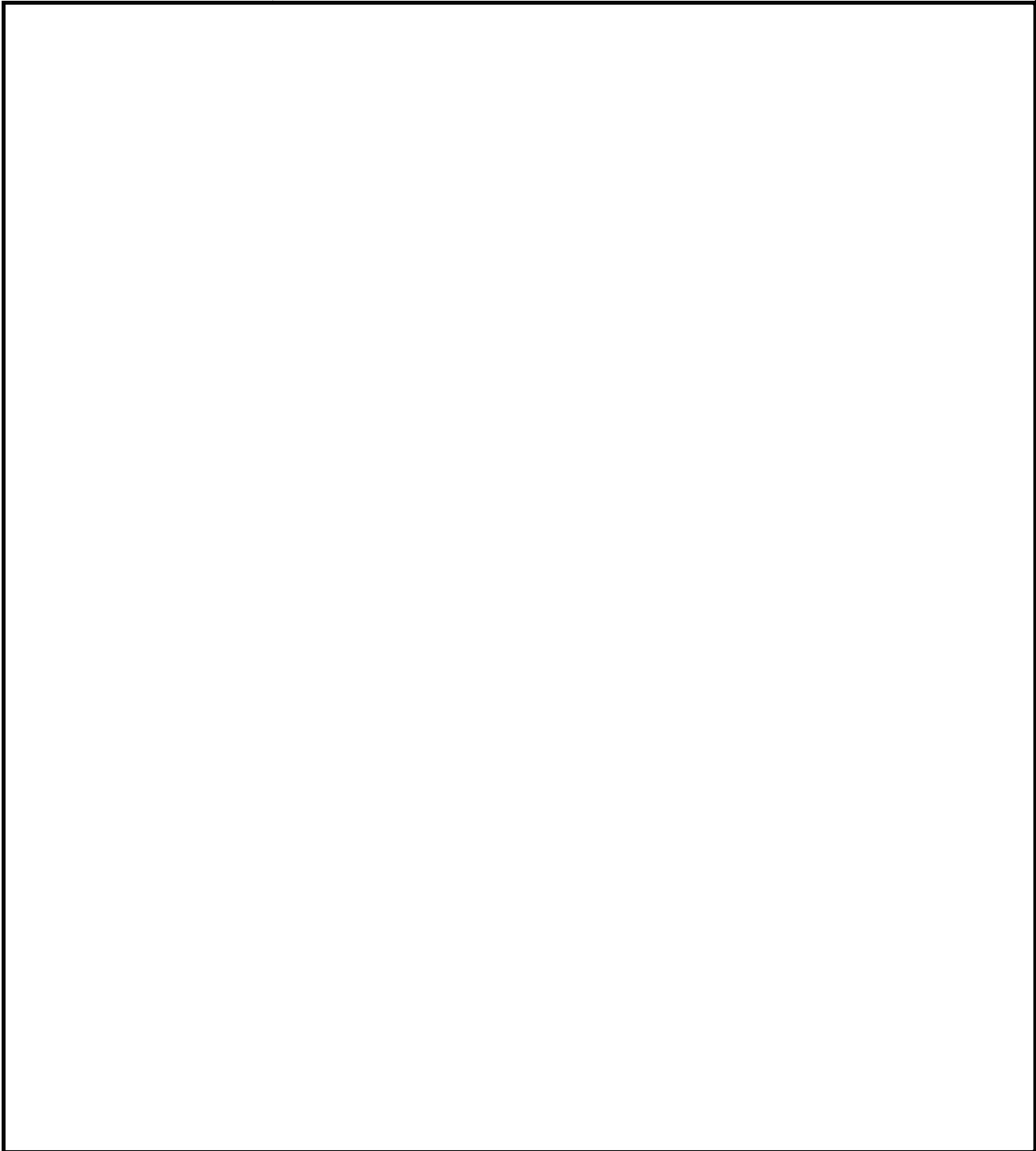
EO 3.3b(3)  
PL 86-36/50 USC 3605



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605



~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

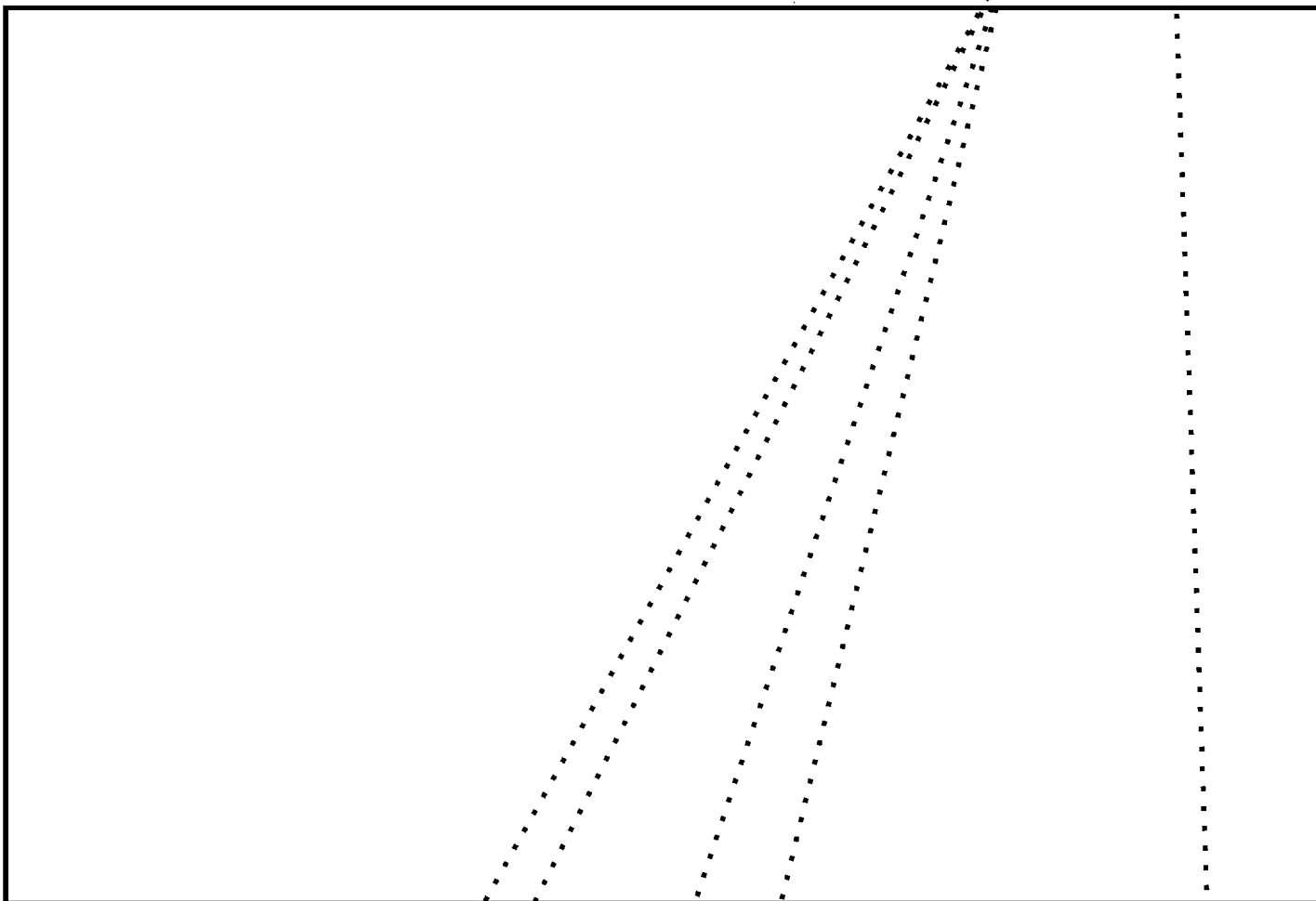
## Wife sells husband

BANGKOK, 27 May—Police at Nonthaburi Precinct Police Station Saturday disclosed a bizarre story to the local Press: A woman came in Saturday morning to file charges "of fraudulent practice" against another woman for non-payment of money after she sold her husband.

According to police, Mrs Somporn Sukhonghapol claimed that Mrs Somthavil Aekchart recently agreed "to buy" her husband at an agreed price of 8,000 baht (about 400 US dollars). Mrs Somporn said she agreed to take 2,000 baht (about 100 US dollars) in cash first, with the rest of the payment in the form of a post-dated cheque.

However, when she went to the bank to cash the cheque Friday it bounced "and Mrs Somthavil refused to settle the payment". —NAB/APF

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

You may ask: "What is this grotesque thing above, fluttering as the page trembles in hand..."

Pulling out the old Thesaurus, we find that it is most often referred to as an insignia, or a symbol, crest, shield, and possibly even a badge. Putting aside the fine printed pages, we find that the definitions fit rather nicely.

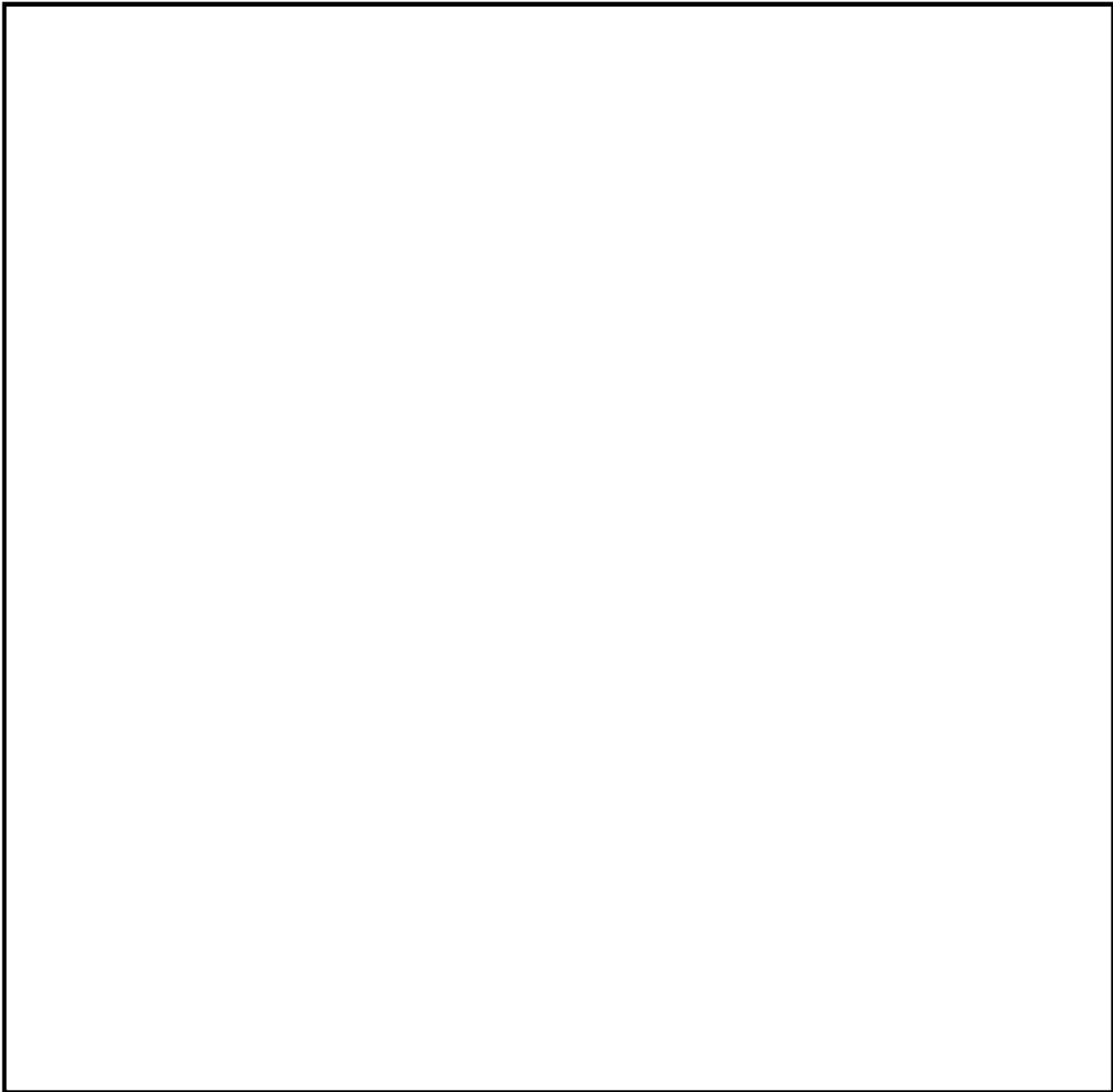
The [redacted] as pictured above, was recently selected by a majority of votes in the [redacted] (B1224) among an enormous four and a half entries to reign as the section's symbol. Whereas each entry contained technical aspects of NSA's policy aiding in the enrichment of the [redacted] lives, the winning emblem, which was conceived and drawn by Sgt Frank Frate, delves into the aesthetics of the country and the people.

Referred to earlier as a grotesque picture, a correction must be made. In black and white, the symbol is misleading; however, as the emblem is posted in B1224, one can easily view the [redacted] [redacted] which symbolize the color and beauty of the country and especially the people.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

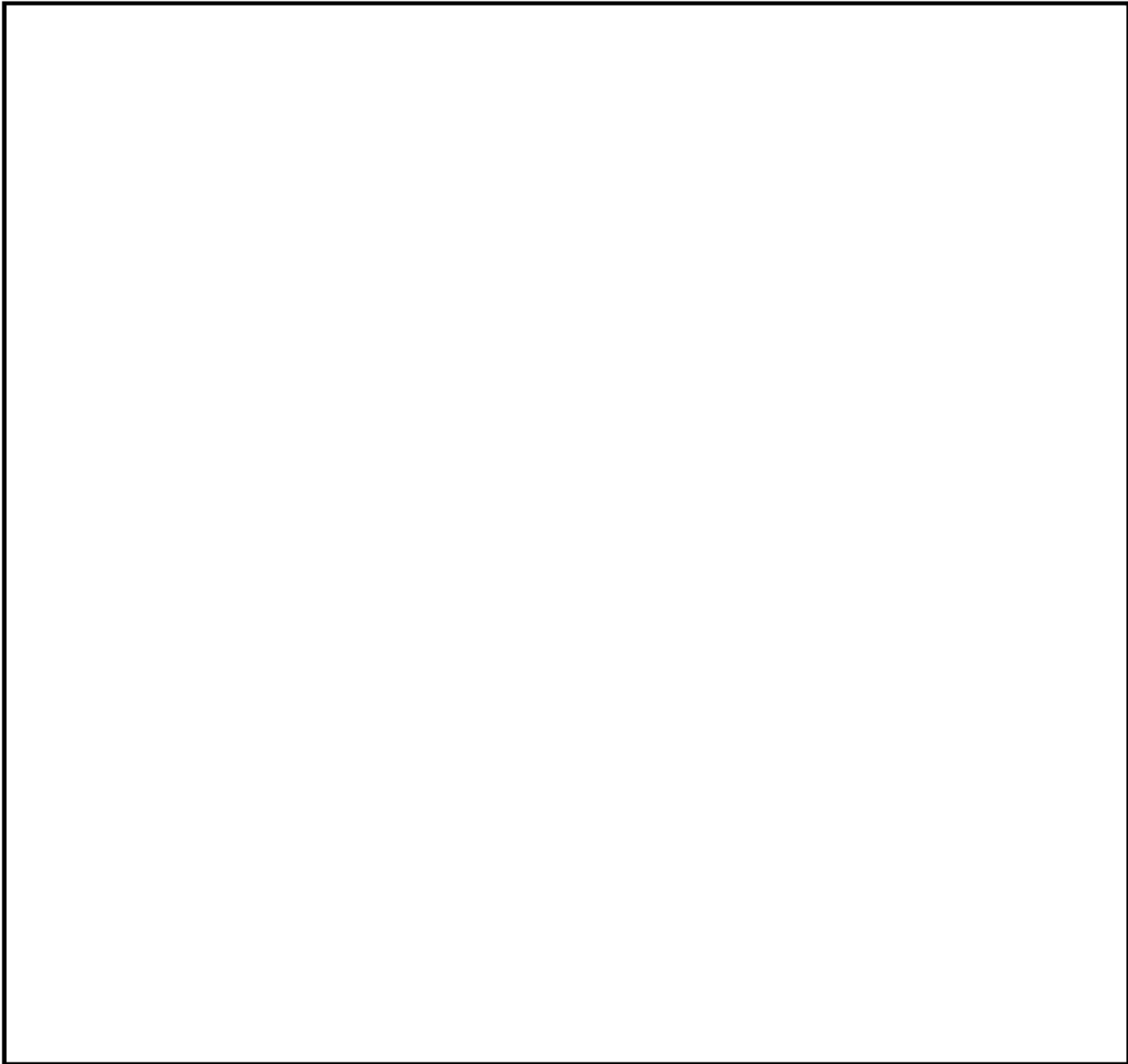
A HITCH-HIKING CIPHER  
by Mary Ann Laslo, B43



~~TOP SECRET UMBRA~~

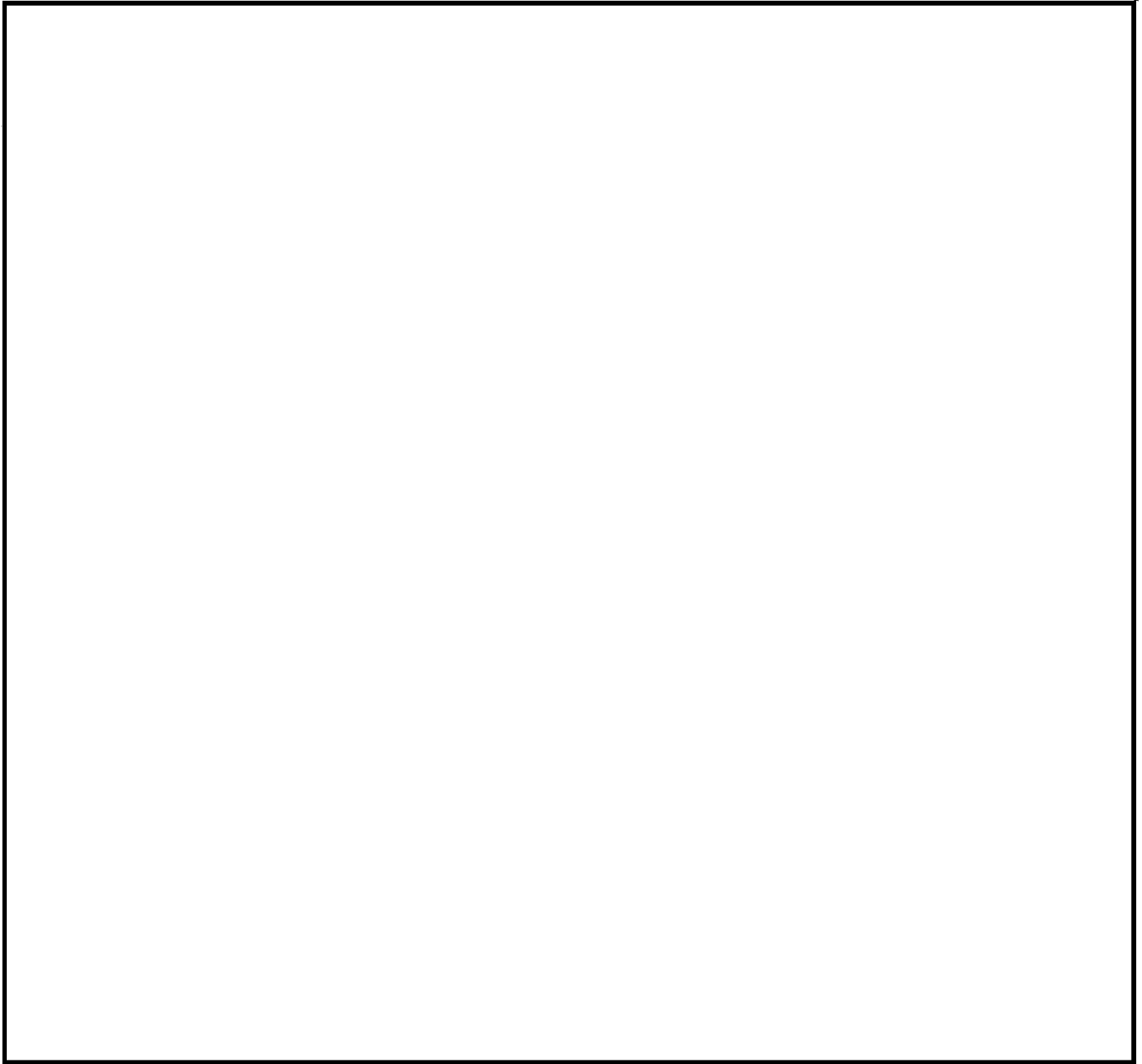
~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605



~~TOP SECRET UMBRA~~

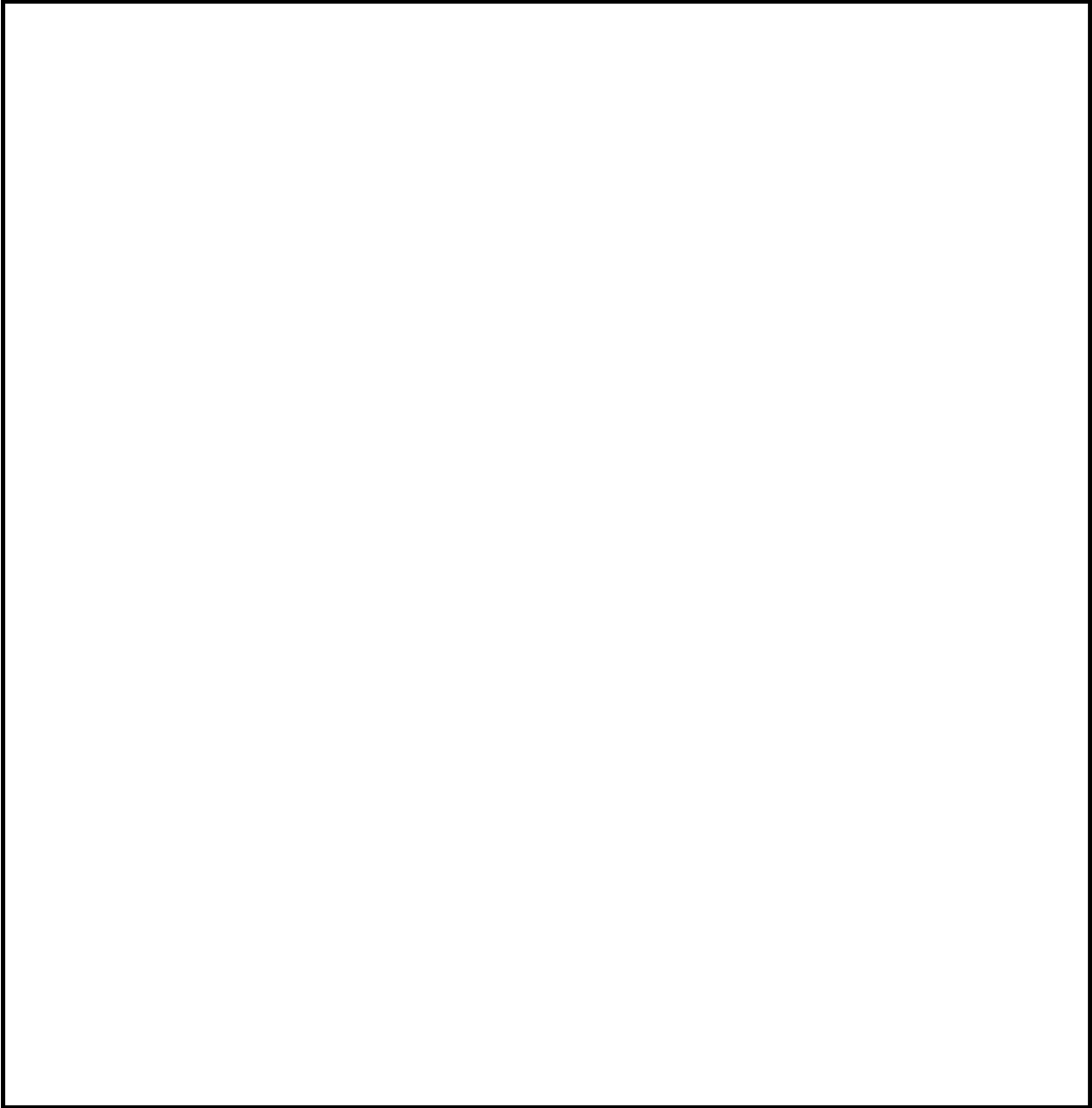
~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605



~~TOP SECRET UMBRA~~

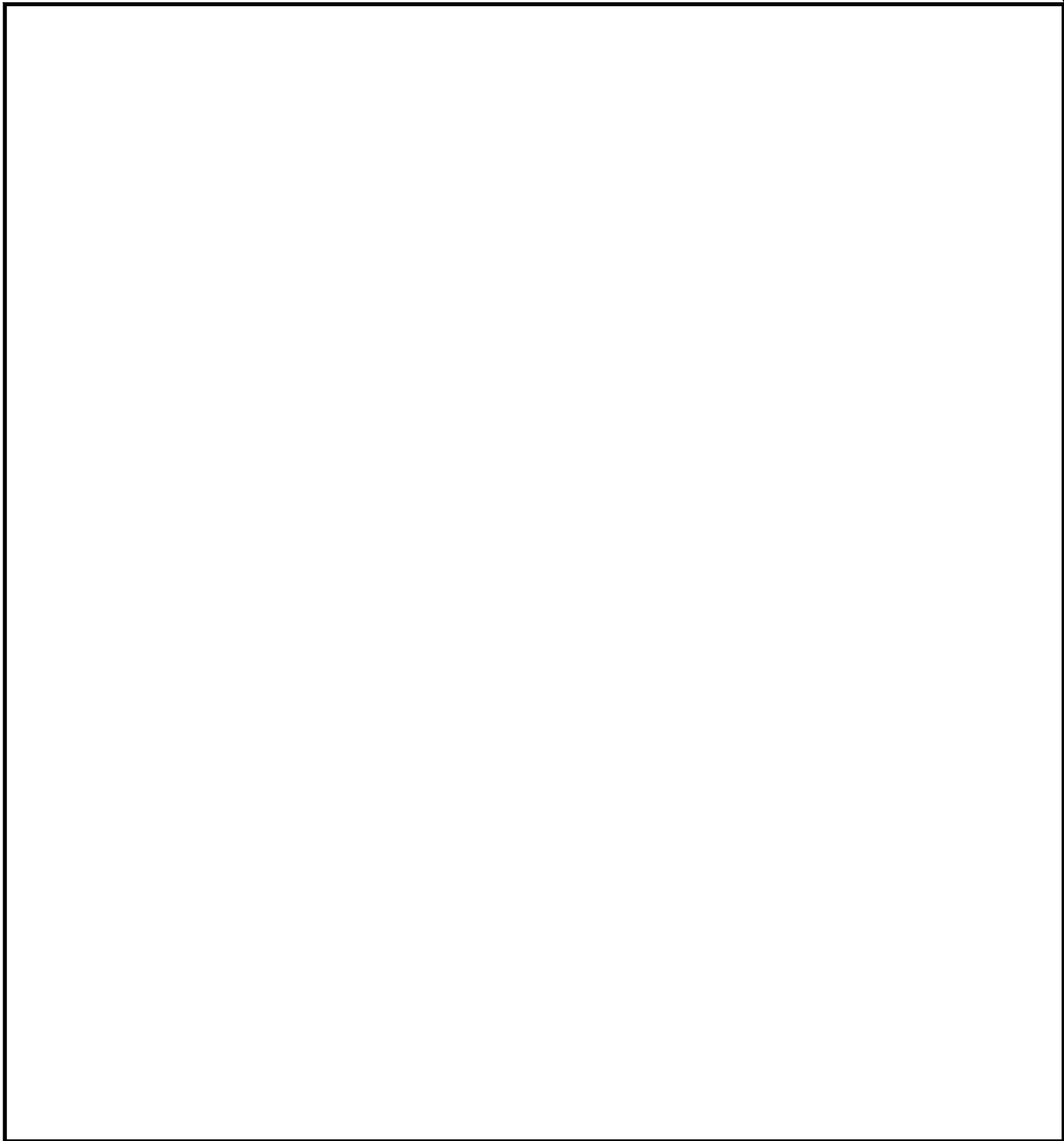
~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

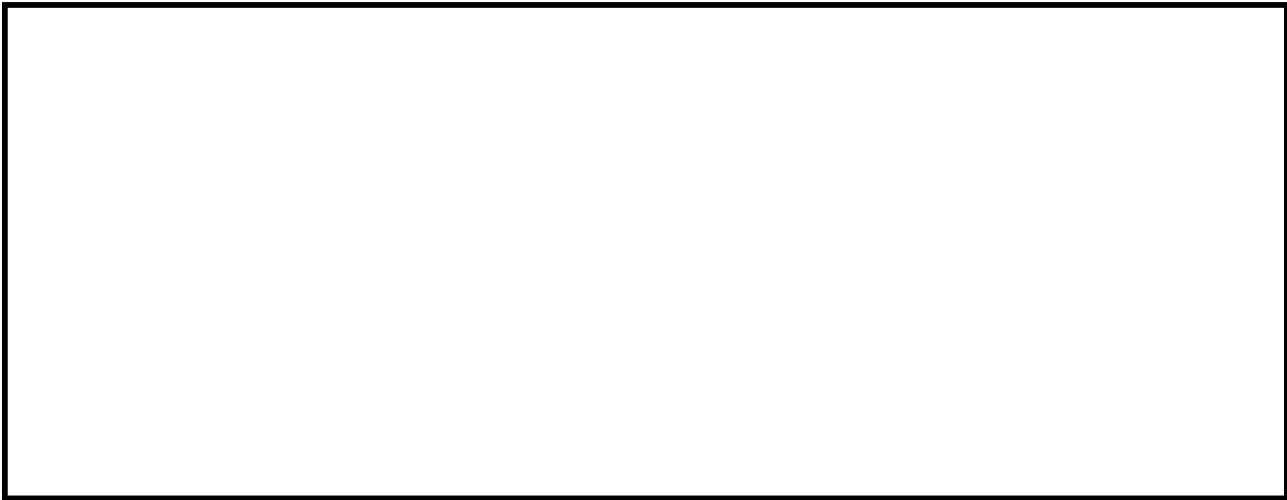
EO 3.3b(3)  
PL 86-36/50 USC 3605



~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~



\*\*\*\*



*A thousand thanks for your articles!*

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

PROBING A NEW TECHNIQUE: CRIB DRAGGING IN SINGLE TRANSPOSITION USING DIGRAPHIC WEIGHTS

by Dr. Marti Branstad, Pl

This is a report on an experimental examination of crib dragging as a technique for breaking into single transposition. Crips of length four were used. Experiments were run using both English and [redacted] For English, digraphic transposition weights were used.

$$w(i,j) = \log \left[ \frac{f_{ij}}{N} \right] = \log \left[ \frac{N^{f_{ij}}}{(\sum_i f_{ij}) (\sum_j f_{ij})} \right]$$

For [redacted] digraphic chained weights were used.

$$w(i,j) = \log \left[ \frac{f_{ij}}{N} \right] = \log \left[ \frac{c^{f_{ij}}}{\sum_j f_{ij}} \right]$$

APPROACH #1:

All possible crib placements were located. For each placement, a sequence of preceding and following quadruples were scored. If a sequence of MINSPAN or more quadruples each of which scored above THRESH was found, it was printed. The next placement was then examined. More formally,

if possible crib placement is  $l_1, l_2, l_3, l_4$

then calculate  $s_i = \text{score}(l_1 - i, l_2 - i, l_3 - i, l_4 - i)$  for  $i=1,2,\dots$

until  $s_i < \text{THRESH}$

then calculate  $s_j = \text{score}(l_1 + j, l_2 + j, l_3 + j, l_4 + j)$  for  $j=1,2,\dots$

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

until  $s_j < \text{THRESH}$

if  $\max i + \max j > \text{MINSPAN}$  then output the quadruples just examined and their scores. Proceed to examine the next possible placement of the crib.

NOTE:  $\text{Score}(a,b,c,d) = w(C(a),C(b)) + w(C(b),C(c)) + w(C(c),C(d))$   
where  $C(a)$  is the cipher letter at position  $a$ .

RESULTS: Four messages in  were processed.

Message No. 1: The cribs were placed correctly and had high scores.

2: The correct placement wasn't found.

3: The correct placement was found but it had a low score.

4: The correct placement wasn't found.

Two messages in English were processed.

Message No. 1: The cribs were placed correctly.

2: The correct placement wasn't found.

APPROACH #2:

The same scoring of quadruples was used. The sum of the scores for SPAN quadruples was examined. The intent was to lessen the effect of any one "bad" combination of four letters in the vicinity of the correct placement. More formally,

for possible placement  $l_1, l_2, l_3, l_4$   
SPAN-1  
calculate  $\text{SUM} + \sum_{i=0} \text{score}(l_1 - i, l_2 - i, l_3 - i, l_4 - i)$

if  $\text{SUM}/\text{SPAN} > \text{THRESH}$  print the result

calculate  $\text{SUM} = \text{score}(l_1 + 1, l_2 + 1, l_3 + 1, l_4 + 1) +$   
SPAN-2  
 $\sum_{i=0} \text{score}(l_1 - i, l_2 - i, l_3 - i, l_4 - i)$

if  $\text{SUM}/\text{SPAN} > \text{THRESH}$  print the result

...

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

(continue calculating and testing the last SUM is  
SPAN-1

$$\text{SUM} = \sum_{l=0}^{\text{SPAN}-1} \text{score}(l_1+i, l_2+i, l_3+i, l_4+i)$$

Proceed to examine the next possible placement.

RESULTS: The approach was used on message No. 3 of [redacted]  
[redacted] It located many "good" placements (SUM>12 for  
SPAN=10); however, it failed to locate the correct placement  
(SUM fell between -5.06 and 1.67 for all alternatives).

CONCLUSIONS: These experiments, done for B1203, seem to indicate  
crib dragging using digraphic weights is an unreliable technique  
for breaking into single transposition. B12 is currently revis-  
ing the weighting and threshold parameters in an effort to make  
this technique work.

\*\*\*\*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

---The new rulings on retirement have hastened the exodus of several of our cohorts. Saying "So long" on 30 June are:

Frederick Stires, B04  
 Margaret Gohrband, B12  
 Thelma Cook, B21  
 Dicey Coyne, B21  
 Mary Talley, B22  
 Chris Christenson, B41  
 Fred W. Johansen, B44  
 Margaret Hickernell, B44  
 Theodore Lively, B44  
 Caroline Flaccus, B45  
 Mary Henley, B61  
 Dorothy Evans, B63

Good luck! Keep in touch! And, remember the Phoenix Society!

\*\*\*\*

---If you're having a bit of difficulty with your AG-22 data base query and response techniques, you may find the series of programs developed by Bill Davis, B2, and catalogued on the 370 the answer to your dilemma. These programs allow the user to make specific SPECOL queries to manipulate the data base as desired.

An interesting example is the program called DF FIX, which is designed to provide a fix list by RAD using line bearings retrieved through SPECOL from the STRUM/

AG-22 data base. Routines are available which allow the user to correct identifications (RADs) and delete unusable DF modules before program fixes are attempted.

For information about other programs in his library, Bill can be reached on 5561s.

\*\*\*\*

---MANAGERS NEEDED--WANT TO APPLY?

The American Management Association, which has sponsored conferences for women managers since 1967, says attendance at these courses has roughly doubled in the past year. "Women are hungry for management education," asserts Rosemary LeBoeuf, a program director for the Association.

Where are the hungry women in NSA? If what we are really working for is acceptance as a matter of course in being considered for and performing any job for which we have the capability, let's become qualified.

The Cryptologic Management Department of the National Cryptologic School and local universities offer programs which emphasize the issues found in most of the new management courses for women: decision making, communications,

~~TOP SECRET UMBRA~~

**TOP SECRET UMBRA**

problem solving and group dynamics.

Here is the real challenge. Do you desire management training? Are you personally willing to invest your efforts to participate in management training? Do you know what is available and what the prerequisites are?

If your answer to the first question is no, forget it. If your answer to the second question is yes and you need answers to question three, call Helen Schmidt, ext 6101. This is the first step in getting your training requirement into the system.

---Be a WINner with WIN---

\*\*\*\*

---B Group Language Coordinator's Office has recently published the second of a series of language aids, entitled, "Handy-Dandy 2." These aids are being compiled primarily for the many Chinese linguists in the Agency who desire to learn or maintain familiarity with terms commonly used. Many military personnel arriving at the Agency from language schools have mentioned a forgetfulness or unfamiliarity with some Chinese characters and instead of fighting their way through "dozens" of former textbooks they want something "handy."

These language aids are not intended to serve as texts, but as guides for vocabulary studies with some Chinese character exercises that should be beneficial for the serious student.

Copies of these "Handy-Dandy" aids have been provided to various B Group Offices, NCSch, incoming Chinese linguists, and to other interested personnel. Suggestions for new language aids are earnestly solicited by B02.

\*\*\*\*

---B12's Project CALLIGRAPHY, aimed at developing a software package capable of reproducing on-line any of the several writing systems encountered in Southeast Asian communications, produced its first usable Chinese character decrypt on 16 April 73.

The idea behind this undertaking is to provide analysts of languages with non-roman alphabets the same services available to other linguists---decrypts, working aids, etc., in the native script. (See *Dragon Seeds* Vol 1, Nr 4, Sept 1972).

Being developed is a system similar to G Group's VICEROY system [redacted]. The significant difference is that VICEROY uses a fixed vector character set which makes it language specific. CALLIGRAPHY is designed for user implemented character sets and is therefore language-independent.

\*\*\*\*

---If you would like to have a copy of Military Cryptanalytics (Callimahos and Friedman) Volumes I and/or II, please call the Cryptanalysis Department, NCSch, on 8-8025. There are a limited number of copies of both volumes available.

~~**TOP SECRET UMBRA**~~

~~TOP SECRET UMBRA~~---TRANSCRIBER BONUS CLARIFIED

The Language Career Panel's 1968 edition of the "Criteria for Certification of Professional Linguists" provided for an additional 100 points under the Language Ability Criterion for "demonstrated ability to transcribe operational voice tapes" (Paragraph IIC). The Panel evolved the following policy governing the awarding of this bonus:

1. Certification as to operational transcriber ability was to be accomplished by the aspirant's supervisor by means of a memorandum to the Panel.

2. Transcriber bonus was to be awarded only in cases where it could be certified that the aspirant was or was capable of transcribing operational voice material.

3. The bonus was to be awarded only after the aspirant had passed the PQE and had satisfied all other criteria minima.

4. Where the transcriber certification pertained to non-current experience only, the Panel reserved the right to require the aspirant to demonstrate his transcriber ability by taking a specially prepared test, the forerunner of Part IIB of the present PQE format.

A number of voice transcribers in the Agency achieved their professional certification in this manner and the procedure fulfilled a much needed escape valve in the certification squeeze for these people.

With the promulgation of the Revised Criteria in June 1972, the procedures for awarding additional points for demonstrated language ability were modified. Credit on the basis of a supervisor's certification was discontinued. The Panel now grants an additional 100 points under the Language Ability Criterion for any one of the following:

a. Exceptional performance on both parts of the PQE.

b. Acceptable (passing) performance on Part I of a second language examination.

c. Acceptable (passing) performance in one additional SIGINT discipline (Part II) within the same language.

The Panel's revised Language Ability Criterion became effective upon publication (12 Jun 72). No grace period was allowed. However, the Panel recognized that some special accommodation had to be made for those aspirants who had been counting on the old bonus when they finally passed the PQE. The Panel modified its policy to continue awarding the 100 points for transcriber ability under the 1968 Criteria until 12 Jun 73 for those who had already submitted such certificates. In extending this provision, however, the Panel ruled that to qualify for the old bonus, aspirants would have to take and pass Part IIA (SIGINT Translation) of the new PQE which equates to the former Part II. Passing Part IIB (Transcriber's

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

option) obviously does not satisfy the intent of the Panel's original policy, for in allowing it the aspirant would receive double credit for the same thing. This point is made here in order to clarify any possible misunderstanding that might arise during the overlap period between the expiration of the 1968 Criteria and the effective date of the 1972 revision.

EO 3.3b(3)  
PL 86-36/50 USC 3605

\*\*\*\*

---Did you know that B is investigating the development of a computer system to provide on-line



\*\*\*\*

---Be sure to read Jerry Gegan's (B12) interesting article in the May issue of QRL to get some insight into the problems connected with training and utilizing military linguists at field processing sites.

ATTENTION BOOKBREAKERS --

"Collected Articles on Code Reconstruction" is the title of a recent NSA publication, edited by Constance Clarke and Kay Swift for collateral reading in the bookbreaking course, CA-301. Anyone wishing a copy may request it through Betty Ames, E13, x8025s, FANX II.

\*\*\*\*

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

\*\*\*\*

---Be sure to read the bulletin titled "College Training Program, Fall Semester 1973" issued by the National Cryptologic School if you're planning to take some after-hours courses next semester. To be eligible for Agency sponsorship (2/3 of your tuition and associated laboratory fees), you must

1. be a full-time (40 hour week) employee.
2. meet the admission requirements of the college or university of your choice.
3. be requesting Agency sponsorship for the first time or have maintained a C+ average in previously sponsored courses.
4. obtain the endorsement of your supervisor or office chief.
5. have no outstanding obligation from previous Agency-sponsored training.

\*\*\*\*

---AACC at Fort Meade

Anne Arundel Community College will increase its commitment to educational service this fall by providing a full program of college courses for personnel attached to Fort Meade.

Designated in Spring 1974 a Servicemen's Opportunity College (SOC) by the American Association of community and Junior Colleges, AACC expects an enrollment at Fort Meade of approximately 2000 in study programs leading to the Associate in Arts degree.

The result of collaboration of the AAJCS with Defense Department Educational agencies, the

SOC program now involves over 100 two-year colleges throughout the nation and is coordinated to provide service personnel easy transfer of credits and continuity of curricula from one college to another.

\*\*\*\*

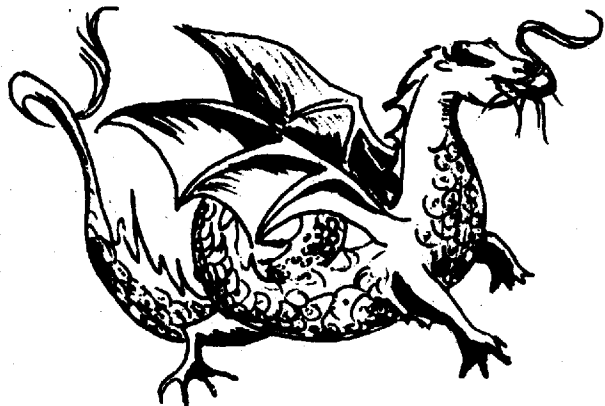
---You computer buffs may wish to mark on your calendars the dates of a series of seminars being presented by Advanced Management Research Inc. on new approaches to solving difficult data processing problems.

The use of microfilm and the development and improvement of microfilm information systems will be discussed at a 3-day seminar to be held in New York City from 16 to 18 October 1973.

An intensive course in systems design and analysis will be conducted in the same locale from 24 to 26 October 1973. This seminar will discuss what is expected of the new analyst and how he can best meet the challenge.

Data base design is the subject of the seminar to be held from 28 to 30 November 1973 in Washington D.C. This course has been developed to give an analysis of the current state of the art of data base development.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

ASK  
THE  
DRAGON  
LADY

A 10 April 1973 memorandum signed by General Phillips states, "The Management Review has indicated that we may have some problems in our manning of linguist...billets. I wish to examine in detail the nature of these problems and the actions we might take to resolve them."

The Dragon Lady submits the following sentiments voiced by some of our senior language analysts in various conversations on the same subject. Opposing or supporting arguments are solicited.

*"The professional linguist at NSA who wants to remain in language work must accept definite career limitations. Except in the rarest instances, he cannot expect to advance beyond a certain point as a linguist. To progress further, he must become strictly a manager--and management is another profession.*

*"That this situation exists is the fault both of higher management and of Agency linguists themselves. Managers tend to think of linguists as interchangeable "bodies." (After all, "Anyone can look up words in a dictionary.") Skill levels, experience, and capability are given only perfunctory consideration. On the other hand, linguists often find their work at NSA so interesting and enjoyable that they are willing to accept, without protest, the lack of advancement opportunities within their field."*

\*\*\*\*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

On the subject of supply and demand:

"We, because of security, are not allowed to compete in the university world; we are not even allowed to compete on an inter-agency governmental basis. Do you think that there is any real opportunity for linguists to sell their talents to the highest bidder? NSA certainly provides no opportunity for us to get together with fellow professionals of other agencies in any situation except under close official observation.

"Free enterprise for government linguists is strictly out of the question. If linguists' salaries are lower at the Library of Congress, at State, at CIA, at FBIS, don't you think it is partly because of this? Once you have worked at one of these places, no one else will touch you. We build our own little empires and never never leave them. But in how many other businesses and industries are you a prisoner of your profession after five years?

"And the fiction that government salaries are so much better than those of the outside world is strictly that.

"I know that many of the better universities have full professor salaries in the \$30,000 to \$40,000 range, which is a very rare thing in the technical, as opposed to the managerial, positions at NSA. And in my view the "pure" professor, as distinguished from the department head, provost, deans, etc., is the professional equivalent of the "pure" technician at NSA.

"What I have said is aimed at the more mundane aspect of our profession (money), but it may help to round out the picture of the linguist's professional situation at NSA."

\*\*\*\*

"When I was a GG-7, I had fantastic personal responsibility. I was responsible for developing the Agency's whole Xendian language program. Then, as a GG-13, I was reduced to counting chairs in classrooms."

\*\*\*\*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

"Languages change constantly. The skills required in language jobs take a lifetime to develop, while those required in the other disciplines are teachable in a short range of time. Language analysts are not given enough incentive to make language work a lifetime pursuit. I'm not sure where the stopping point is. In the middle ranges (GG-7 to GG-13), there is a reasonable career. But, beyond that, it's questionable if enough incentive exists to keep people in the field. And then, we're stingy with our training. There is no overall long range training program in terms of the needs of the Agency and the needs and capabilities of the person.

\*\*\*\*

"As long as promotion above a certain level is on the basis of management, there will always be a shortage of technicians. This is true for other disciplines, too. Not taking anything away from management, but there are other skills that are just as critical to our mission."

\*\*\*\*

"It is wisdom to know others;  
"It is enlightenment to know one's self."

---Lao Tzu

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

T H E W I S D O M O F T H E C H I N E S E S A G E

23 11 4 25 14 20 3 18 16 19 9 24 12 5 2 13 15 17 6 21 7 22 1 10 8

1	T	O	M	E	N	D	B	U	T	T	F	A	I	L	X	E	Q	U	I	T	N	C	E	R	I
2	C	I	U	S	O	H	E	R	E	W	B	Y	T	H	E	Y	X	C	L	E	G	H	T	E	O
3	N	E	D	O	C	A	S	N	O	D	P	E	O	P	L	A	N	G	O	V	U	S	N	E	S
4	T	R	I	N	E	I	V	I	N	E	E	X	X	M	E	E	R	N	M	E	S	A	N	D	C
5	W	A	S	S	A	R	I	G	H	T	N	C	I	U	S	N	T	X	C	O	O	N	S	C	I
6	C	R	E	D	X	O	F	K	I	N	H	E	L	D	T	O	P	E	R	A	E	N	C	E	W
7	X	I	T	H	A	G	S	X	T	H	H	A	T	T	H	T	I	O	N	F	E	R	E	I	N
8	D	C	O	M	E	E	U	N	F	I	E	G	E	N	E	O	R	P	U	B	N	A	T	E	I
9	D	O	W	N	F	T	A	M	O	N	R	A	L	W	E	L	I	C	I	M	N	M	A	N	X
10	R	O	M	R	E	G	W	H	O	M	L	F	A	R	E	P	R	O	V	E	X	T	H	E	I
11	M	O	T	E	A	S	H	O	U	L	O	F	T	H	E	M	E	N	T	X	M	P	L	I	C
12	N	T	I	Q	U	D	B	E	R	E	P	E	O	P	L	A	N	D	L	I	A	T	I	O	N
13	I	T	Y	X	X	M	O	V	E	D	E	W	A	S	A	B	E	R	T	Y	B	E	I	N	G
14	R	O	Y	A	L	B	Y	T	H	E	B	O	V	E	A	O	F	C	O	M	T	H	A	T	M
15	G	O	V	E	R	N	R	E	Q	U	L	L	E	L	S	M	E	R	C	E	O	R	A	L	L
16	N	M	E	N	T	A	L	S	O	R	E	X	X	H	I	X	X	H	E	H	A	W	I	S	O
17	W	A	S	A	N	X	S	H	O	U	S	V	O	I	C	E	L	D	T	H	N	E	W	I	T
18	I	N	S	T	I	L	D	T	H	A	E	W	A	S	U	A	T	B	E	N	H	C	R	E	A
19	T	U	T	I	O	T	P	R	O	C	P	L	I	F	T	E	V	O	L	E	T	I	O	N	X
20	N	O	F	G	O	E	D	U	R	E	E	D	F	O	R										

Solution to March trans-  
position Puzzle.

Answers to Crypto-Scramble:

Cryptoanswer:

Delta I.C.  
Monograph  
Average I.C.  
Sigmage  
Tables

ANAGRAM

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

## CONTRIBUTORS

WALTER D. (JOE) ABBOTT, JR., B605, received his B.A. in English literature from Harvard College in 1960 and entered the Army Security Agency shortly thereafter. Among his Army experiences were a year in Monterey studying Chinese-Mandarin and a two-year tour in the Philippines as the OIC in the Processing and Reporting shop for the now defunct USM-9. He joined NSA in 1966 and had a tour in Hawaii, during which time he was the NSA Pacific representative to the CINCPAC IGC working group. A certified Special Research Analyst, he is currently the Chief of the Intelligence Staff for all Communist Ground Force activity in Southeast Asia.

PEGGY BARNHILL joined NSA in 1966 after graduating from Marywood College with a degree in Social Studies. While a participant in the Special Research Intern program, she worked in various areas throughout the Agency. Upon completion of that program, she was assigned to B42, where she has been deeply involved in development of the software for processing AG-22 data. She is professionalized in both Special Research and Data Systems career fields.

DR. MARTHA A. (MARTI) BRANSTAD, P1, entered NSA as a Crypto-Math intern in 1971. She has had tours in R, C, and B. It was while touring B12 that she isolated several "bugs" in the 370/STETHOSCOPE, a series of C/A diagnostic programs. This discovery led to her present undertaking--that of revamping and debugging the whole RAPIDS (general utility program) package. Dr. Branstad's background includes a PhD awarded by Iowa State University, where she briefly served as Assistant Professor of Computer Science. Even now her ties to the academic world are not completely severed, for after hours she teaches at the University College of the University of Maryland.

RODNEY FORBES majored in English at Notre Dame and Ohio State, where he received his M.A. in 1951. After a stretch in the Army, he kicked around graduate school at Ohio State for a while, studying and teaching, before joining NSA in 1957. He has spent almost his whole Agency career in B Group, having

TOP SECRET UMBRA

**TOP SECRET UMBRA**EO 3.3b(3)  
PL 86-36/50 USC 3605

worked on the [redacted] problem and the CHICOM [redacted] and Development problems. But he has spent more time on the CHICOM [redacted] where he is now serving another tour. With Sally Keil, he published a long TSR (B43 #1-71) on the same subject as his Dragon Seeds article.

WILLIAM D. GERHARD has been with NSA since 1952 except for a two-year period from 1962 to 1964, when he worked for the Science Information Office of the National Science Foundation. At NSA, he has divided his time between G and B Groups--in G as a linguist, cryptanalyst, and reporter and in B as a member of the B6 Operations Staff (1964-65) and the B6 Technical Support Division (T/A, C/A, and machine support) from 1965 to 1967. Since then, he has headed a small NSA/SCA team chartered by DIRNSA to document the U.S. cryptologic involvement in Southeast Asia. Bill received his education at Indiana University, which granted him B.A. and M.A. degrees.

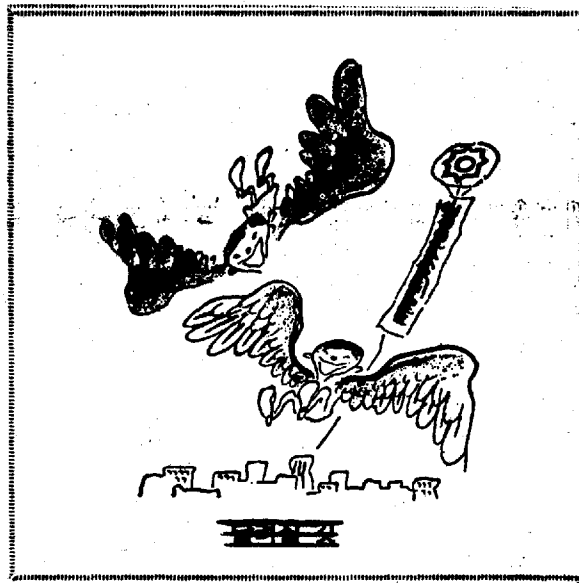
BEE KENNARD, P2221, graduated from the University of Texas with a B.A. in History and English. For seven years she served as an intelligence analyst with G2, U.S. Forces in Austria. From 1967 to 1971 she worked with the B2223 collocated information support group as the senior analyst on the Vietnam Military problem. Currently, she is a "retired war correspondent" and author-in-residence.

MARY ANN LASLO, B432, was graduated from Rosary Hill College, Buffalo, New York, in 1965, receiving a B.A. degree in Mathematics. She came to NSA in 1966 and entered the C/A Intern Program, which provided opportunities to work in A55, B45, G41, and G42. She received her certification as a mathematician in 1970 and as a cryptanalyst in 1973; and she has completed several requirements leading to certification as a crypto-mathematician. Since 1969, Mrs. Lazlo has been assigned to B432, where she does independent cryptanalytic research on the Peoples Republic of China [redacted] and functions as a consultant in mathematics and statistics at Division level.

~~**TOP SECRET UMBRA**~~

~~TOP SECRET UMBRA~~

保  
密



it's classified!!

~~TOP SECRET UMBRA~~



*Vince Wilson, E5*

~~TOP SECRET~~

# National Security Agency

Fort George G. Meade, Maryland



SEPTEMBER 1973



# DRAGON SEEDS

THIS DOCUMENT CONTAINS CODEWORD MATERIAL

~~TOP SECRET~~

~~TOP SECRET UMBRA~~

This is *Dragon Seeds*.

There is fantasy, irony, and the bite of reality in the name. It speaks of the East. And, like the East, it suggests much, says little.

*Dragon Seeds* is both Mother China and her neighbors. *Dragon Seeds* is monumental and minuscule. It is the past and future. It begs for elaboration but gives none. In it are echoed softly slurred Mandarin, brittle Vietnamese, determined Korean. In it is the spectre looming over the Thai, Lao, and Khmer. It is frightening and friendly. It is uncertain.

Above all, *Dragon Seeds* is promise. It is fertile with ideas unbounded, to be cultivated with creativity and imagination. It is challenge. It is alive. It will be more than it is.

*Dragon Seeds* is yours. May it grow with you.

The Editors

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



W  
E  
R  
E  
  
S  
O  
R  
Y

WE ARE LATE!  
REORGANIZATION  
MADE US

M I S S T H E

DATE.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

## DRAGON SEEDS

Publisher

DONALD E. MC COWN, CHIEF B4

Managing Editor

Minnie M. Kenny

Executive Editor

Robert S. Benjamin

Rewrite Editor

Jane E. Dunn

Special Interest Editor

Ray F. Lynch

Feature Editor

Robert F. Kreinheder

Education Editor

Marian I. Reed

Composition

Rita L. Cashwell

Beverly McAdoo

Louella M. Ertter

## PRESS CORPS

B11 Carolyn Y. Brown

B42 Peggy Barnhill

B2 George S. Patterson

B43 Mary Ann Laslo

B31 Jack Spencer

B61

B32 Jean Gilligan

B62 Edmund J. Guest

B33 Louis Ambrosia

B63 William Eley

B41 James W. Schmidt

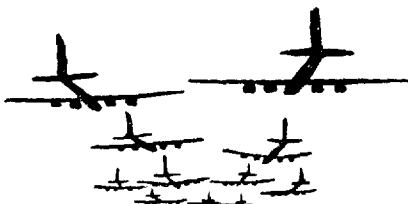
B65 Philip J. Gallagher

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

**Rebels threaten  
Cambodian city**

**Rebels Build Up  
Pressure Near  
Phnom Penh**



**Heavy  
Fighting  
Resumes**

**Battle for Kompong Cham Renewed**

**Insurgents Enter  
Kompong Cham,  
Are Driven Out**

**Siege Eased**



LEA SEN HOEUYI

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605



Vol. 2  
Nr. III

SEPTEMBER 1973

TABLE OF CONTENTS

Buddha Speaks		1
SAWTOOTH Answers the Q Question.....	Jane E. Dunn	8
What Have They Done to Our Linguists?.....	Jeryl O. Gegan	14
The Open Door: Teacher Very Funny.....	Rich Atkinson	19
Surveying <span style="border: 1px solid black; display: inline-block; width: 150px; height: 1.2em; vertical-align: middle;"></span> Cryptosystems..	Sam Coury	24
History of a Dragon.....	Don DeLong	29
Seedlings		33
Ask the Dragon Lady		36
Contributors		41

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



STU BUCK

*. . . receiving the Meritorious Civilian Service Award*

*from*

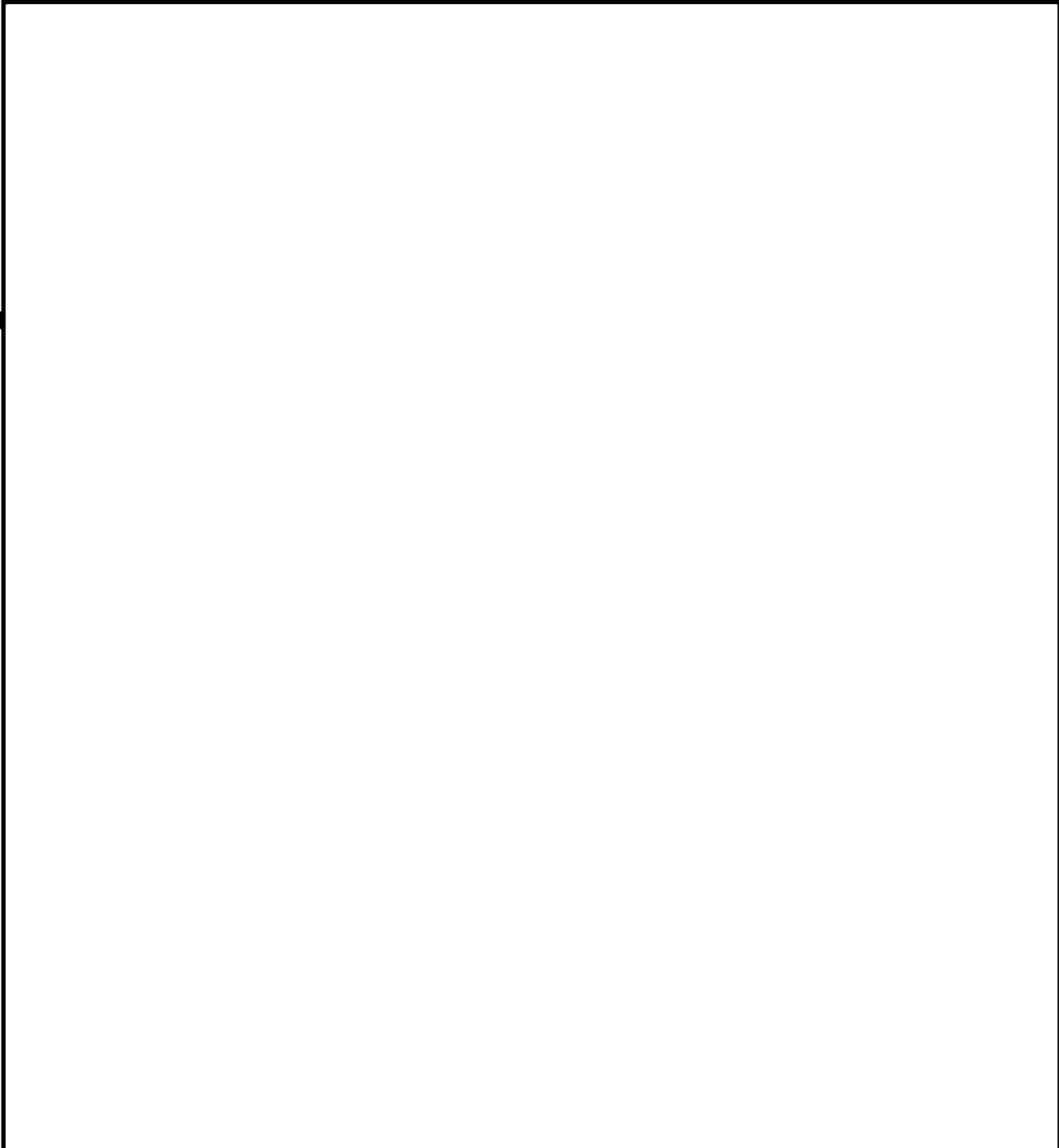
*Gen. Sam Phillips,  
former Director, NSA*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

*B*

COMPUTER-AIDED BOOKBREAKING (NOT "BOOKBREAKING BY COMPUTER")  
By Stuart H. Buck

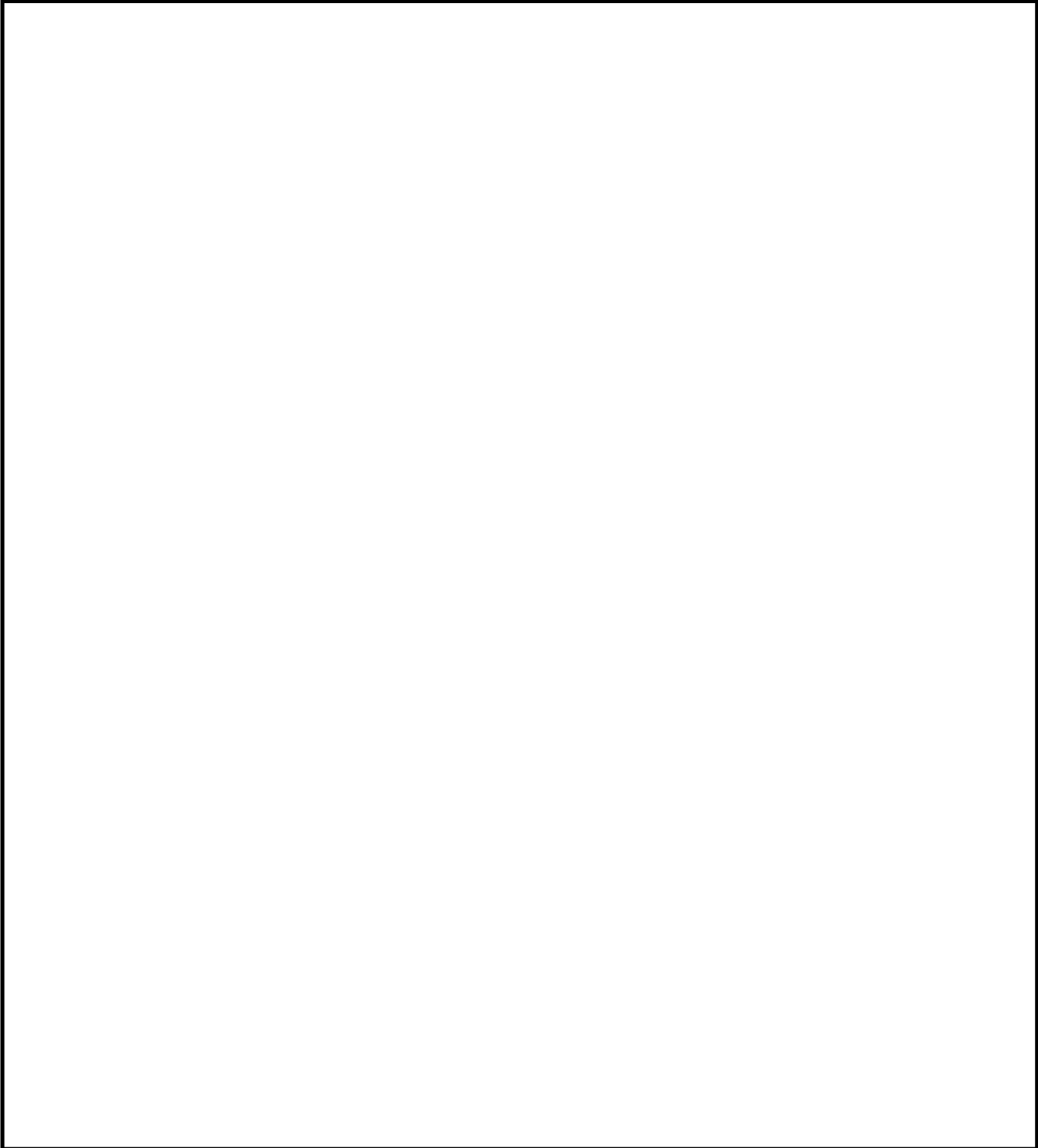


~~TOP SECRET UMBRA~~

*TOP SECRET UMBRA*



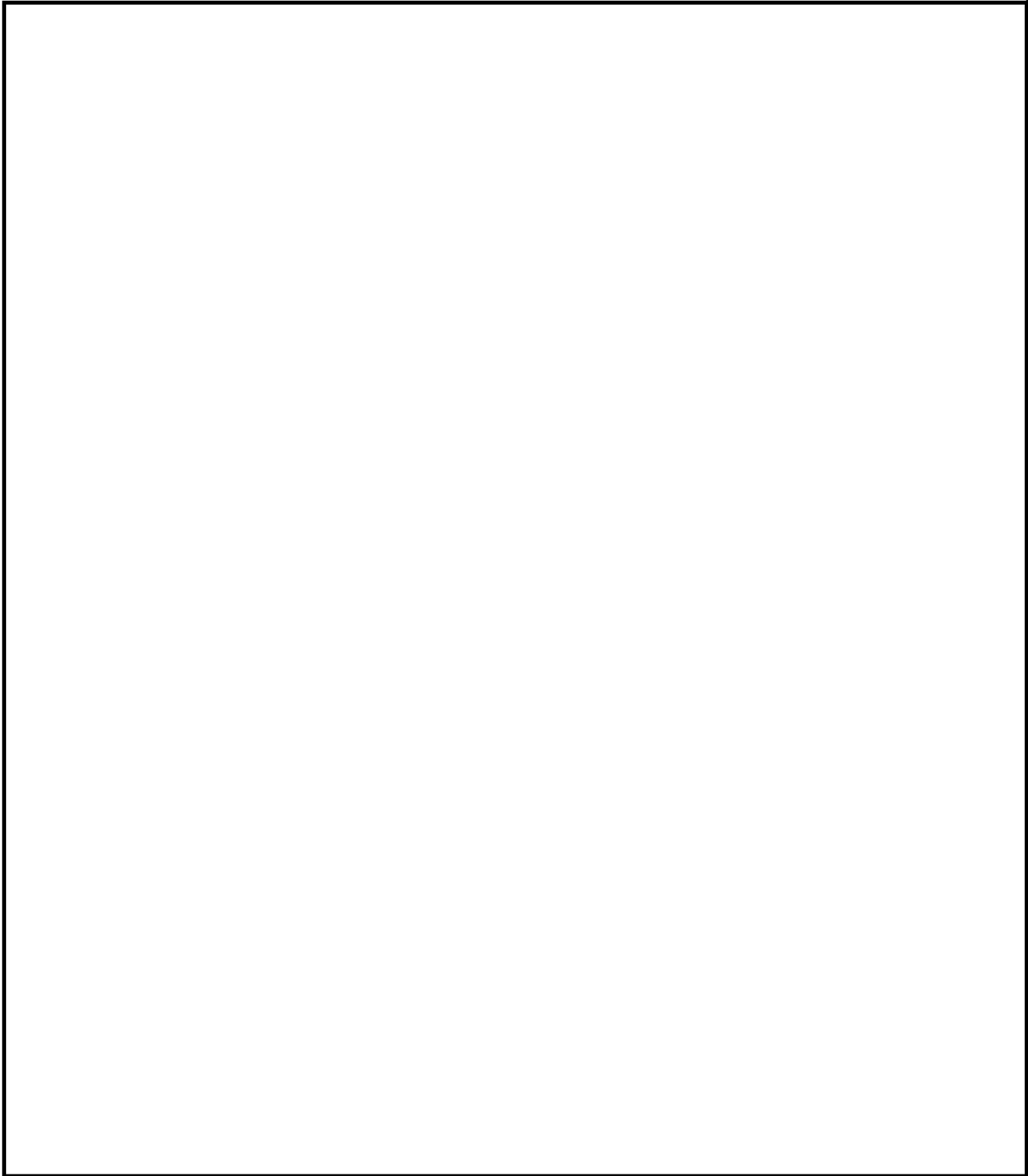
~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

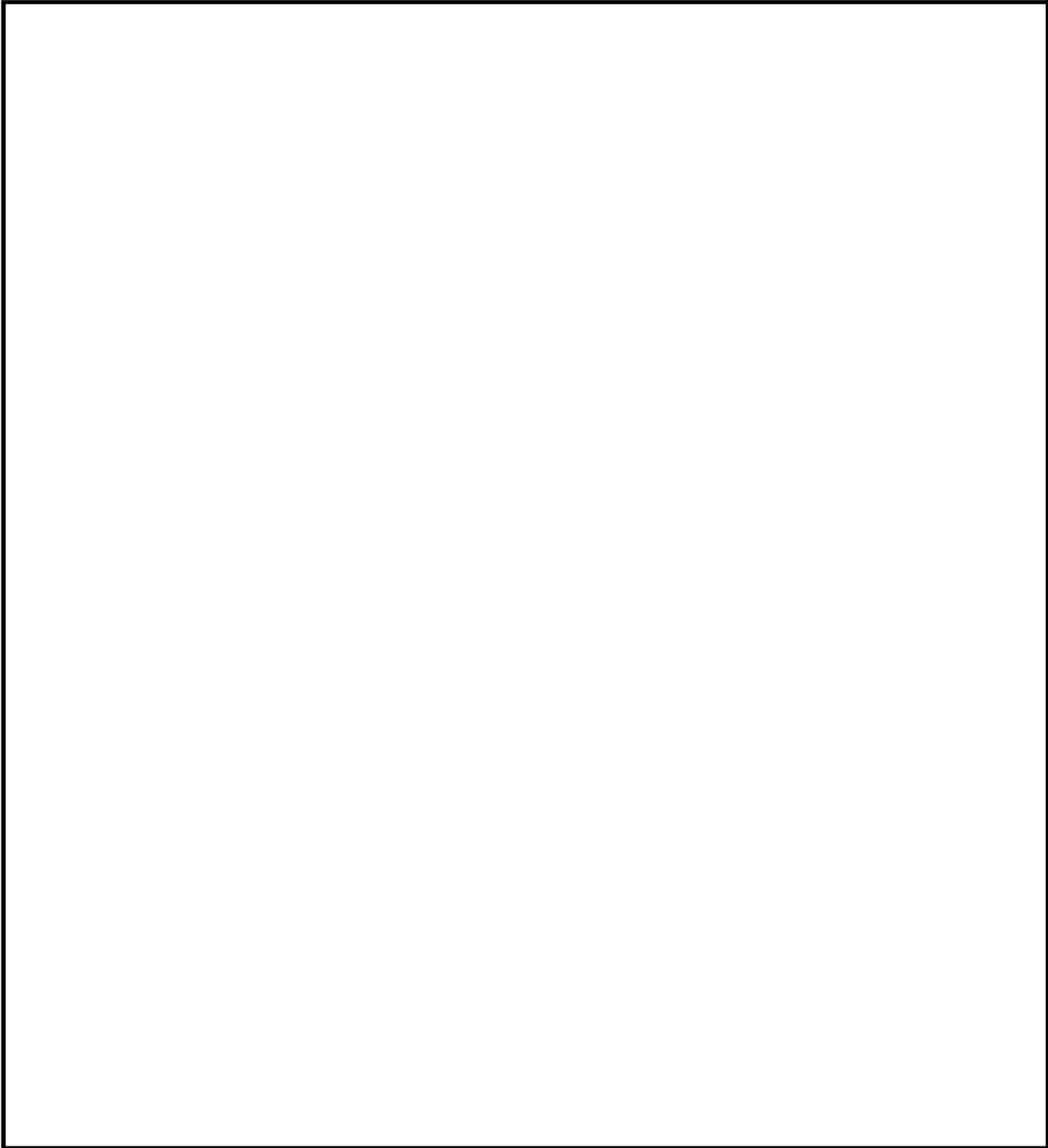
~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

STUART BUCK'S  
 academic degrees reflect major  
 interests both on and off the job;  
 he holds an AB in Romance Languages from  
 Harvard and an MA in History from Columbia.  
 As a history buff, he has made extensive  
 studies on the American Civil War,  
 although his interests range  
 far beyond that one period.

MR. BUCK  
 entered the SIGINT field while  
 with the Army in 1943, and he became  
 a civilian analyst the following year; he  
 has been with the Agency ever since.

Cryptolinguistics  
 was his field from the beginning  
 with concentration on bookbreaking,

Readers of the  
 NSA Technical Journal  
 will recognize him from his  
 scholarly articles on languages  
 and cryptolinguistics, and others know  
 him as the author of handbooks, dictionaries,  
 and readers in  
 Mongolian and Tibetan.

He is deeply involved in developing  
 technical aids to bookbreaking and  
 rejoices in the challenge of working with  
 machine-oriented friends to unite the divergent  
 fields of  
 natural language and computer  
 programming for code reconstruction.  
 Mr. Buck made P1 his base when it was first  
 established as NSA 064 during the Korean War.

\*\*\*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

This puzzle, a Mao quotation in STC encrypted by means of a 10 x 10 playfair, was submitted by SSG Anthony Zambito, B213. It will probably be a "snap" for someone with a Chinese language background but a non-Chinese crypticist could recover the pseudoplain if he were familiar with the properties of STC.

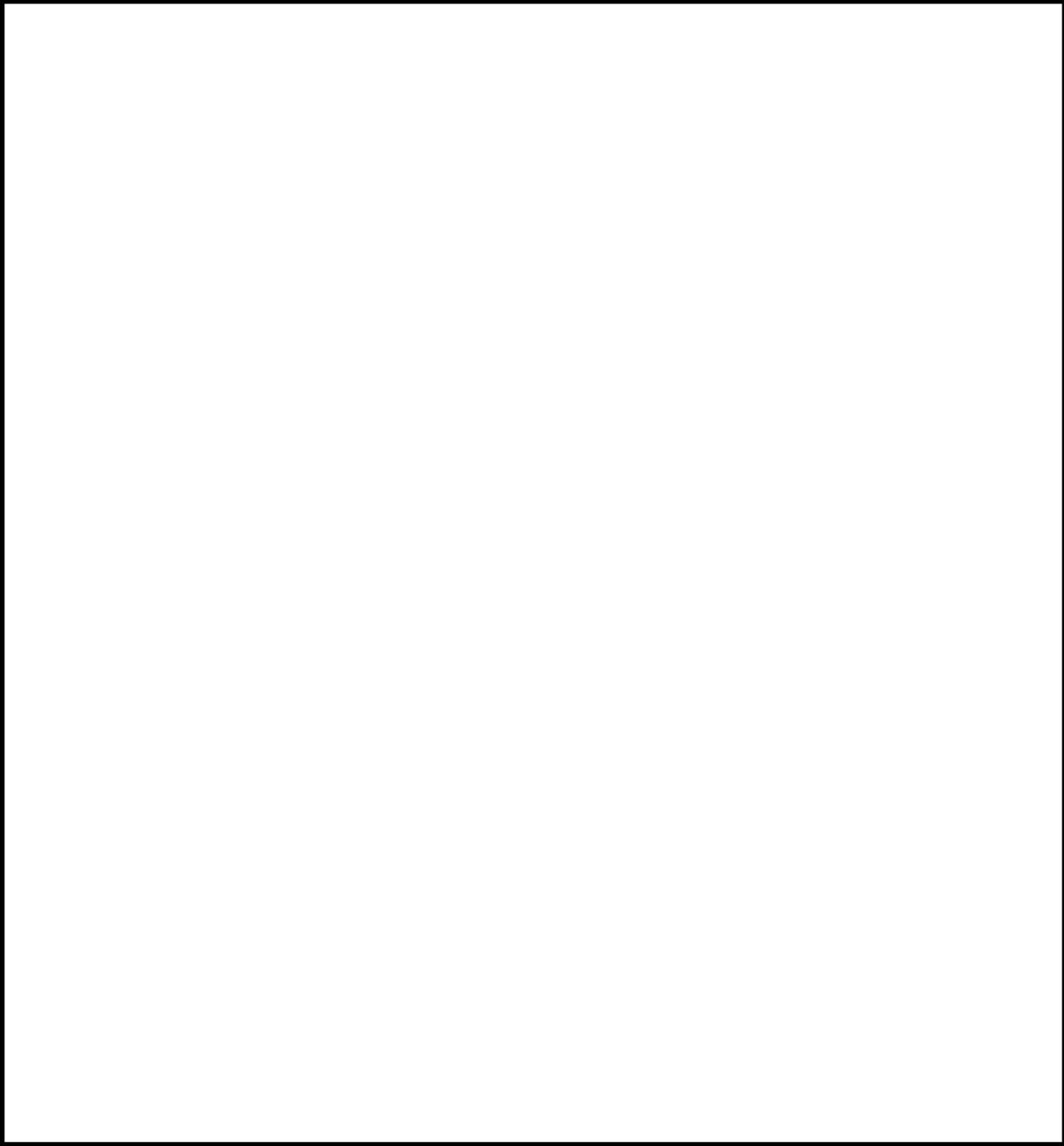
09269	70418	99795	69489	09262	93983	03172	21126
11727	56794	89160	44436	32817	35250	89798	40184
02521	56216	24328	14381	11261	17275	67948	91604
44363	28122	36034	21126	13873	08414	09255	94813
61562	32601	87112	61172	75679	39073	52508	95472
01032	85111	26422	40324	02529	72593	72155	10019
87188	90679	84018	49489	15621	62454	72010	32851
11261	62448	58155	10019	87188	90683	03318	19390
29113	35181	69777	17154	38749	48913	26077	12057
81695	45527	80972	59372	94895	45527	80162	44858
94894	68713	93153	95455	27809	72593	72948	91539
54552	78016	24485	89489	22360	01541	43532	13084
64506	31718	70735	25089	02522	78016	24112	67984
61849	39073	52508	90252	27801	62401	20112	61604
54704	65695	14948	92210	76513	27677	61735	25089
20722	78016	24207	21126	87188	90677	42318	10157
66294	27494	89327	67761	73525	08902	52278	01624
11264	67017	79015	76629	42749	48989	40010	32210
76515	01127	24298	80426	11261	17248	14015	76629
42749	39010						

(Answer in next issue)

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

SAWTOOTH ANSWERS THE *Q* QUESTION  
by Jane Dunn, B4



~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~

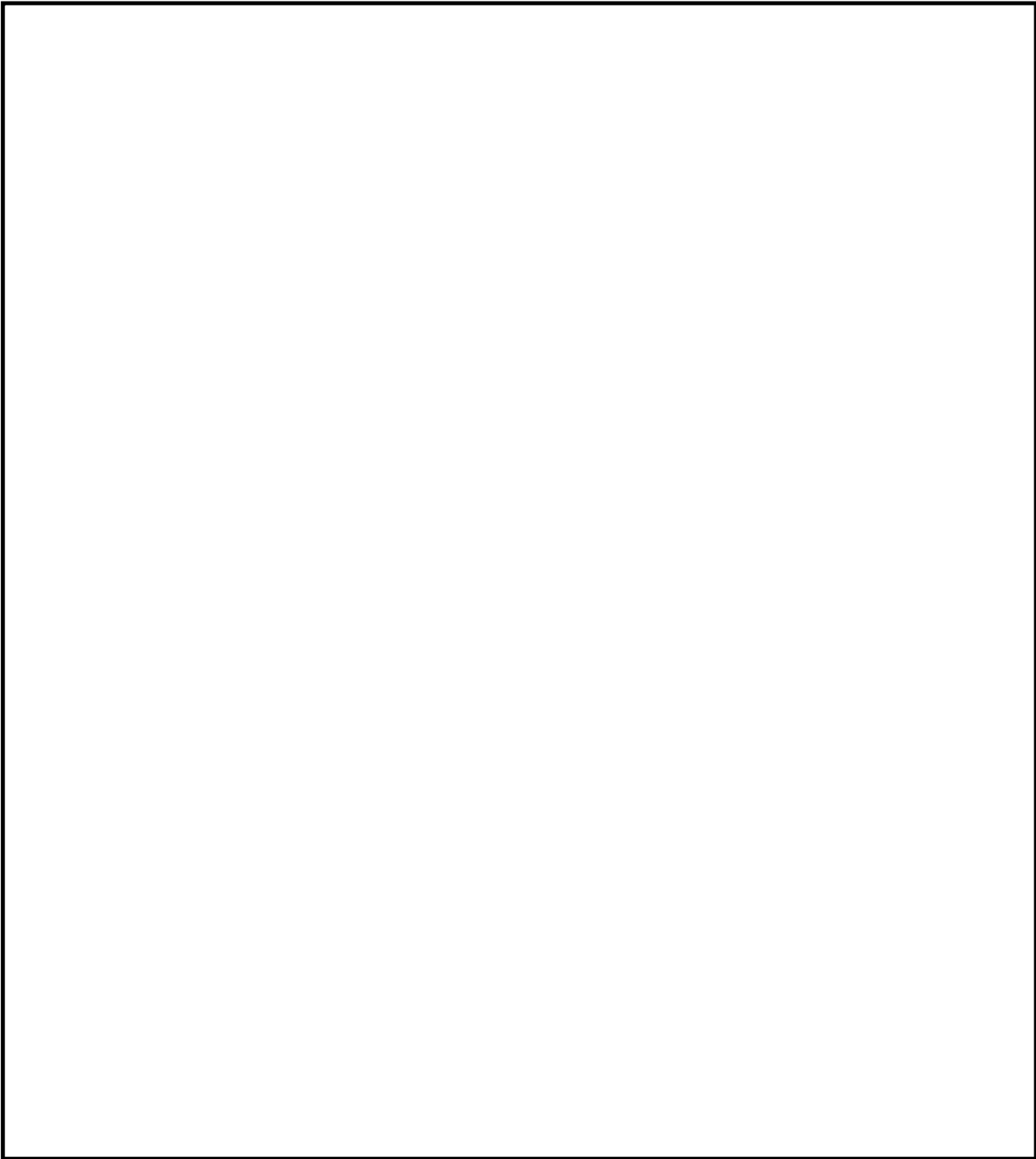


~~TOP SECRET UMBRA~~



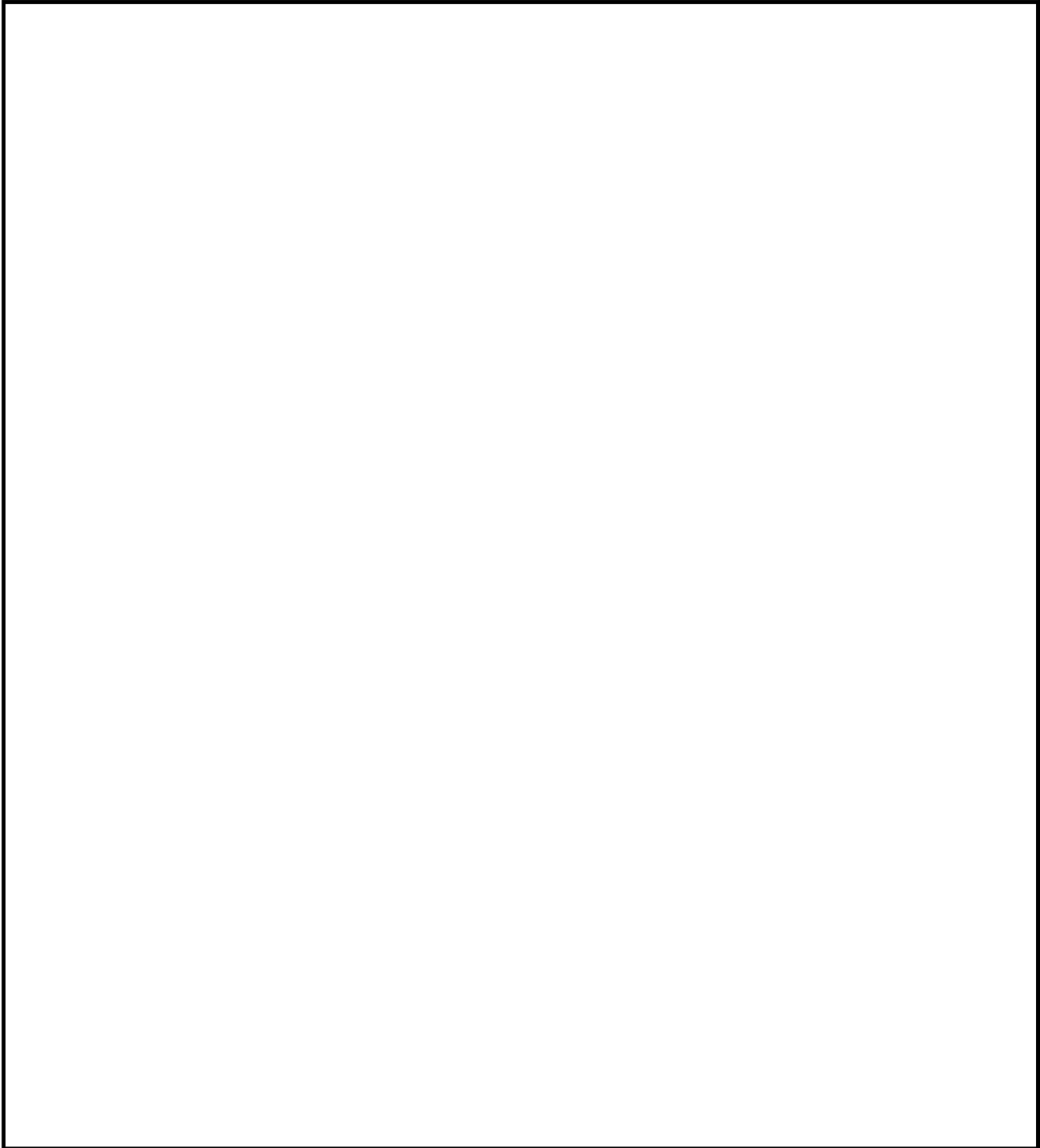
~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605



~~TOP SECRET UMBRA~~

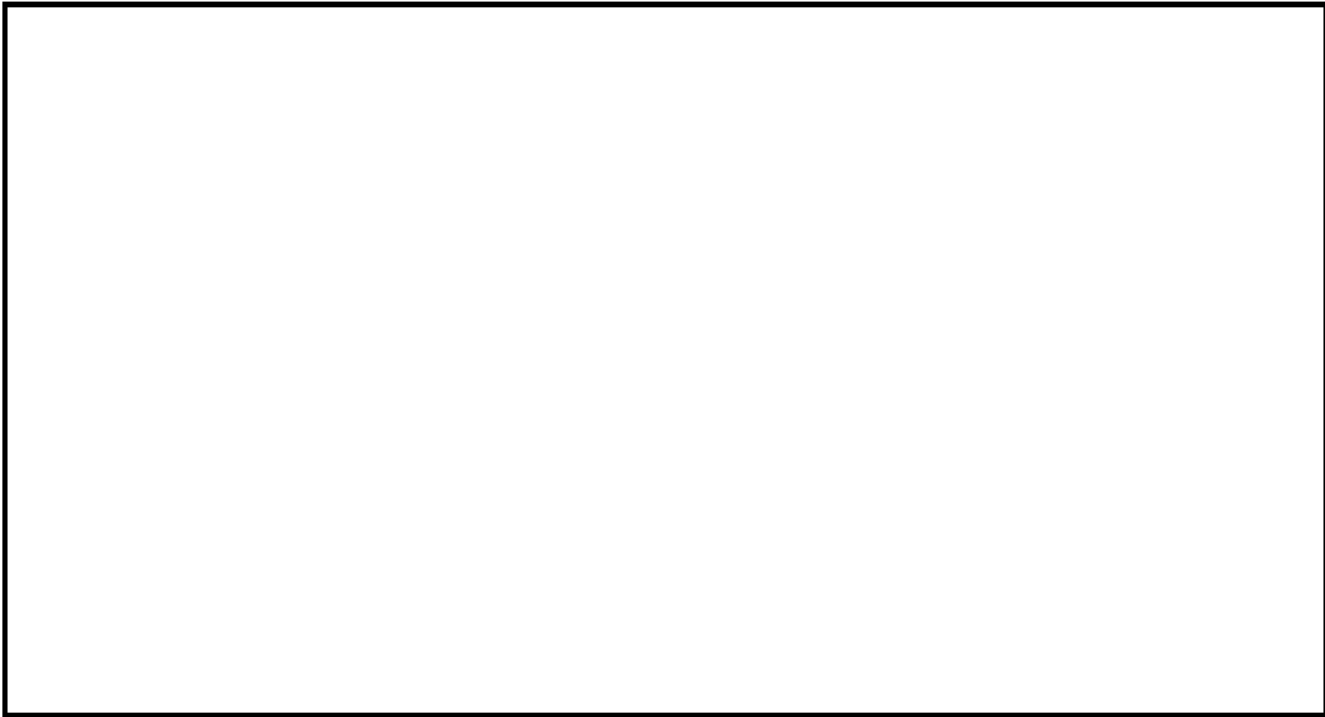
~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

11/11/2001 10:11:11 AM

~~TOP SECRET UMBRA~~



\*\*\*\*

*"We will*

*Make a new*

*Garden*

*More splendid*

*Than this one.*

*You will see it*

*You will understand . . ."*

*--Chekov*

~~TOP SECRET UMBRA~~

# ~~TOP SECRET UMBRA~~

## CRYPTO-SCRAMBLE

By Richard Atkinson

Unscramble each of the five numbered crypto-scrambles, placing one letter in each space, to form five words or names, each of which fits the definition to its right.

1. T R A C E I S G R E E N  
○ ○ ○ \_ \_ \_

A set of decipherments.

2. M E T S T E P  
○ ○ \_ \_ \_

COMSEC worry.

3. V I T A L S E A B E E R  
\_ \_ ○ \_ \_ ○ \_ \_

Converted by addition of a constant.

4. W H O S A D  
\_ \_ ○ \_ \_

RYE program performs statistics on data stream and its delta stream.

5. P U R E T E S T S  
\_ \_ \_ ○ \_ \_ \_ ○

RYE programs of pure tests.

Now arrange the circled letters to form the cryptoanswer suggested by the cartoon at the right.

Print CRYPTOANSWER here.  
\_ \_ \_ \_ \_



Answer on page 40

~~TOP SECRET UMBRA~~

WHAT HAVE THEY DONE TO OUR LINGUISTS?

By Jeryl O. Gegan, B65

The other day I received a Notification of Personnel Action slip telling me that my job title and COSC had been changed from Special Research Analyst to Language Analyst. Panic -- (There must be some mistake!) -- was followed by despair. Who would do such a thing to me? How will I ever face my friends and co-workers? This can't really be happening to me! After recovering a few of my senses I began calling all over the Agency to find out why I was being persecuted. . . . I called my personnel representative, the Career Guidance Division, and one of the B Group Technical Directorates. Most of the time I couldn't get through to my party; either the lines were tied up by other erstwhile SRA's who also had just been retitled or possibly no one wanted to talk to a mere language analyst.

REFLECTION

That night, alone and crying in my beer, I began to reflect on what had happened to the image and status of linguists in this Agency. When I started in the cryptologic business nearly ten years ago, my first assignment was as a linguist. Ah, those were the good old days! A linguist was *somebody* then! A linguist could walk around the halls of NSA or a field station and try to appear indifferent to all the admiring glances he received. He was the man on the spot with all the responsibility, all the answers. Whenever VIP's visited to be briefed on the tactical situation, the political situation, or on any other situation that needed looking into, the linguist was *it!* He was the leader of all who needed leading, the brightest star in all the firmament.

But, alas, the golden age has passed. The white knight image has been shattered. A new animal has appeared on the scene. He will lead the blind, cure all ills, and answer any questions. He is: "The SRA."

Since the Vietnam war has been blamed for everything from inflation at home to the shortage of raspberries in Portugal, we can conveniently blame the war for the tarnishing of the image of the linguist. During the golden age you couldn't find any SRAs; reports and analysis were handled by linguists when they weren't busy translating. In those days, the volume

TOP SECRET UMBRA

~~TOP SECRET UMBRA~~

of translatable items was much less than it is today. Translations didn't need explanations, observations, elucidations, or provocations. It was all there in black and white; only a dummy couldn't understand what it meant.

#### REJECTION

Then the war began and message volumes mushroomed until linguists were confronted with huge backlogs. Additionally, all messages had to be carefully and fully translated -- even the most mundane could contain a wealth of information about enemy plans. Each message had to be viewed as just a tiny piece of the war. Suddenly, nothing was black or white anymore. Someone had to take all the information these messages contained (or possibly contained), and put it into a form which the by now very confused customer could understand and then act upon. The linguists busy working on their backlogs, had no time. So, a new creature, the SRA, emerged to unravel the customers' confusion and save the entire war effort. The SRA assumed all the glamour roles. He issued the CRITICS, the Spot Reports, and the TACREPs. He was responsible for issuing the SONGBIRD TACREP which would result in a downed pilot being plucked to safety right from under the enemy's nose. He drew flags all over the maps. He knew where all the friendly and enemy positions were. He was both a military tactician and strategist. He knew the enemy commanders by name, age, and place of birth. If anyone had any questions or needed a briefing, his supreme excellence, the SRA, was the giver of all truth. The linguists, meanwhile, were still working on their backlogs. The only time anyone talked to a linguist was when the veracity of a translation was questioned. In that rare moment of actual human contact, the linguist didn't know how to act. He hemmed and hawed and sometimes reverted to his acquired language for safety and comfort. Alas! The day of the linguist had passed. He had only one unromantic mission -- to get that backlog depleted.

#### RENAISSANCE

One day during the height of the war, a linguist crawled out from under the table where he had fallen while checking the 17th dictionary for the meaning of an obscure term and discovered that another world, one that he vaguely remembered, really existed. He saw people writing reports, in English, of all things! He saw people giving briefings flanked by gaily-decorated wall maps. He felt a twinge for the past and, right

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

then and there decided that this was for him. One by one, other linguists defected until the Agency had acquired a bevy of SRA's with extensive language capabilities. The "new improved SRA" was born. He could write, brief, analyze, explain, and talk about the idiosyncrasies of the language. He could sooth the restless inquisitive mind of the tactical customer, telling him not to worry, that in this or that instance, the enemy didn't really mean what he said.

Armed with all this versatility, the "new improved SRA" looked for new worlds to conquer. He scooped up jobs handled by traffic analysts and cryptanalysts. He started hanging around with programmers. He took MP-160 and began discussing inputs and outputs. This gave birth to the "vastly improved SRA" whose thirst, still unquenched, slipped into management and staff positions where he could exert influence over all the other production skills. His pride and mobility were unstifled and he had no desire whatsoever to return to the caves and consult a foreign language dictionary.

NOW WHAT?

Although the above story is obviously in jest, I'm sure many linguists are going to recognize the paths their own careers have followed. Why should someone spend a lot of time and effort on the thankless task of producing a translation when the only reward is the question, "Why couldn't we get this out a little sooner?" The feeling among many linguists is that they have absolutely no mobility in the Agency. An individual feels that there is no way he can progress if he remains a linguist. He must graduate into management or expand to other fields, generally SRA or Traffic Analysis. For proof, how many division chiefs with a language analyst COSC do you know? Would he be in the same grade level if he had remained a linguist?

The NSA Language Career Panel, comprised of highly dedicated professionals, has worked diligently to improve and insure the quality of linguists at NSA. With the continuous changes and improvements being made in the Professionalization Qualification Examinations, grading methods, and professionalization criteria, the Panel's mission toward high quality linguists is being realized. But, very little is being done to improve the image of linguists. They are looked upon primarily as units of energy which are expected to produce X number of translations a day. If and when the translation backlog is depleted, they can work on some innocuous language working aid. The Cryptolinguistic

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Association gives these downtrodden people something to join, somewhere they can find a little sympathy and exchange experiences, but this organization is not causing any great change in the image or status of linguists either.

The R&D types are heralded for devising wonderful machines to collect vast quantities of raw data over incredible distances. Traffic analysts score major breakthroughs in locating and identifying terminals, developing comprehensive norms, and solving the mysteries of unit subordination, etc. Cryptanalysts and their data systems compatriots use computer technology to shatter the toughest of ciphers and codes. But, where would we be with all this data were there no linguists to translate? Simply put, it would be a raw and cursory data explosion, neither justifying the cost nor the limited amount of external intelligence information derived. On the other hand, one tiny, taken-for-granted, unrewarded, immobile linguist can make it all worthwhile. He has done it, and because he has, this Agency is recognized among many customers as somewhat of a miracle worker.

In my opinion, there are several reasons why the linguist has been downgraded. Most of the individuals in the other production professions seem to feel that the linguist's job is not "technical" enough. Tough TA and CA problems may take months or years of trial and error studies until the big break comes, but even the toughest translation can be finished off in a relatively short period of time. Reporting requirements demand it. Real-time and near real-time reports must be written up and sent out immediately, but the SRA can also write long-term reports which when completed are masterpieces of intelligence information -- not a stone left unturned, every end tied up. The SRA can express his knowledge in deciding how a report will go out, what vehicle, what precedence, who should get it. He is generally familiar with the other intelligence agencies and the people who work on his problem there. The SRA goes to meetings and NIEs to talk to these people and to customers; his is a glamour job. So then, these other professionals look upon the linguist as someone who after a year to two (or seven or eight for Chinese) of language training, can sit down and translate anything. It's as simple as that. The linguist's job just doesn't *seem* technical enough for him to be held in high esteem.

As if that weren't enough, too many of our linguists enjoy the life of a scholarly recluse. He hides behind his mound of dictionaries and is oblivious of anything else that is going on around him. He holds the other professions in contempt, refusing to see how they could possibly be contributing anything of value.

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

Too often when something does occur that could expand his level of understanding and application in the other cryptologic fields, he will crawl into the woodwork with the excuse that it's not language-related and therefore no concern of his. He'll even hint that he's being misused and that his job doesn't include non-linguistic work. Maybe it doesn't, but all this complaining we hear about lack of mobility and opportunity ought to be looked at in another light -- who is really at fault?

The concept of a superlinguist has been promoted by some. This theory holds that instead of a linguist moving into management or staff work after gaining non-linguistic experience in other cryptologic specialties, he should proceed to gain versatility in as many languages as he can. The more languages he knows the higher he goes, until his job, as a GG-15, is to check translations done by many junior linguists. This, to me, is the height of nonsense. Why have a GG-15 do a job that a GG-9/11 could probably do just as well? This concept promotes shirking of responsibility and encourages retreating behind an even higher mound of dictionaries while the rest of the world goes by. Could this be how the "rejection" phase started in the first place? A concept such as this will do even more to isolate and immobilize an individual.

Everyone is going to have to do a little to help improve the image of linguists at NSA. Remember! Where would this Agency be without them? Perhaps management will have to initiate a course of action, but the big change is going to have to be in the individual linguist himself. Linguists should stop hanging around the wailing wall, stop looking for sympathy from their fellow linguists, and stop blaming everyone but themselves for their '*maligned condition*'. The linguist, if he is to regain his status among other cryptologic professionals, is going to have to take it upon himself to accept more responsibility, expand his technical understanding, and learn a little bit more of what this Agency is all about. To do otherwise will be to conclude that the image of the linguistic profession at NSA has nowhere to go but down. The image is that of the individual.

\*\*\*\*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
EO 3.3b(6)  
PL 86-36/50 USC 3605



### THE OPEN DOOR

*We seek to be companions along the way.  
The lantern which we carry is not ours.  
The spirit which we share is contagious thought;  
The knowledge which we gain, an illuminating torch  
And all who seek may perceive and learn.*

-The Concept of Dragon Seeds

TEACHER VERY FUNNY

by Rich Atkinson, El.

April and May of this year I spent with the [redacted] Advisory Detachment in [redacted] to conduct a six-week course in cryptanalysis for a class of [redacted] NCO's. I could probably write a small book about my two months in [redacted] but this article is limited to my experiences which relate to the course and my relationships with the students.

I'd been in [redacted] a week or so when the first day of the course dawned. I slept later than I had since arriving - almost 5:00 a.m. To be honest, I never did adjust to the [redacted] time differential. I arrived at the center where the course was to be conducted about an hour early and reviewed the "hot tips" I had received from various people:

1. my English-speaking students were not too English-speaking [seems fair, I only knew two [redacted]]
2. [redacted] disappear for a few days at a time and for no particular reason [this could be a nightmare];
3. [redacted] school day is 9-11:30 and 1-3:30, if I'm very lucky [double nightmare];

EO 3.3b(3)  
PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
EO 3.3b(6)  
PL 86-36/50 USC 3605

4. never ask [redacted] a question he can't answer because he will lose face, so it is best not to ask any questions [if they do show up, I can't find out how they are doing];
5. teachers are treated like gods [I have always admired honest emotion].

Armed with the helpful hints, I marched off to battle - me against [redacted] students and a [redacted] acting as interpreter. After rather stiff and formal introductions, I decided to start the class by telling it some of the things they would be able to accomplish after the course. I also hoped this would relax the students a bit. It appeared to work very well; students began to laugh and chatter among themselves. I knew I was off to a good start. Then the Major wiped his eyes and said, "Every student think teacher very funny". My spirits sank to a new low. The remainder of the morning went quickly, and my confidence was coming back because I felt, we were making some progress. But I still needed an icebreaker to open up a good relationship with the students.

When I returned from lunch, I discovered hot tip #2 had already reared its ugly head. One student was missing and when I inquired as to his whereabouts, I was told, "He go to post office. It far away; we start." Well, we not only started the afternoon session without him; we finished it without him. If attendance continued on this "optional" basis, the course would be worthless. I considered the episode as a possible challenge and mounted a counterattack. I told the class I was very impressed with their afternoon work. They were obviously pleased with the compliment. Then I added that they understood so well that they could help the missing student catch up before class began the next day.

As I walked to class the next morning, I didn't know what to expect. My hopes rose when I saw that all five students were present. I chatted with the student who had missed the afternoon session, and he assured me that the other four students had taught him all the material he had missed. There were no more mysterious disappearances during the course.

Next day I found my icebreaker. I had learned from one of the [redacted] advisors that the students wanted to know how old I was. When it was time for our morning break, I put on my most serious face and asked, "Who wants to know how old I am?" The room went silent and six bodies froze. Fearing I'd been a bit overdramatic, I smiled and said, "I'm 33."

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

[redacted] burst into laughter and almost fell off their chairs. I asked for a translation of the chattering. The Major regained his composure and said, "They think teacher very funny." Indeed it was the icebreaker and at least once a week for the rest of the course they would point to my graying hair (almost unknown [redacted] and ask again. The answer, 33, remained amusing for six weeks.

After a few days, I discovered a way around the "losing face" problem. I would ask a student a simple question. When he answered I immediately asked each of the other four students whether the answer was correct. Needless to say, the other four always agreed that it was. If the answer was correct, all five students were pleased; if not, the first student didn't lose face because everybody missed it. Great idea, but I'm glad I didn't have 30 students. By the fourth or fifth week, I was able to call on students and discuss their answers without checking with the other students.

Another ploy used to gain their confidence and overcome the "losing face" problem was to have the class teach me a [redacted] word each day. I think it was the highlight of their day to hear tone-deaf me attempting their tonal language. Since I didn't appear to lose face with my performances, perhaps they felt they couldn't lose face in front of me.

Before anyone gets the impression I was able to convert [redacted] students into typical Americans let me stress two important points. First, these men weren't typical [redacted] and [redacted] were aware of my American idiosyncrasies. Second, those recounted were my only two "victories". I gave in on all other clashes of customs. For example, wild horses couldn't drag a student out of the classroom before the teacher. On breaks I often wanted to write something on the blackboard before my next lecture. They wouldn't go on break until I left the classroom. My only recourse was to go out and sneak back in a few minutes later. During the morning and afternoon breaks, they wanted to buy me Cokes. One day I decided to break them of this rather expensive habit. During exercises, I sneaked out and bought myself a Coke. I came back to class with the full bottle in my hand and suggested a break. Thirty seconds later, I had a bottle of Coke in my other hand and the student who brought it to me marveled at the tremendous thirst I had. I capitulated. They had to erase the blackboard; they had to carry my notes back to my office; and no amount of protest altered a thing. There was give and take on both sides, and we each learned something about the other.

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
EO 3.3b(6)  
PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~

By the second week of the course, the students realized they could learn the subject matter, and hot tip #3 bit the dust. All students were in class by 8:30 each day and studied until I appeared at 9:00. They returned from lunch about 12:15, and studied or did exercises until I appeared an hour later. By now lessons had become a real pleasure for me, eager students full of questions and willing to learn - a teacher's dream. Deadlines went out the window - if exceeded fine, if not, [redacted].

Occasionally we went to lunch as a group. These meals consisted of many different courses of chicken and seafood washed down with liberal amounts of [redacted] the local whisky, or beer (good but potent). Each course comes with a special sauce or two. Using these sauces, [redacted] food extremely hot. Mexican food seems like a bland diet after [redacted]

During the fourth week, I decided to take the class to lunch and asked a [redacted] advisor for the name of a local restaurant. He recommended one where the food was good, but he wanted me to know it was a [redacted] restaurant not designed for tourists. Just what I wanted - not ostentatious and cheap. The day before we were to go, I had the Major announce the invitation. The class was agreeable, but not overly eager. We went the next day. After a somber beginning, we all had a great time and rolled back to class a couple of hours later. When one of the students took me aside to thank me, I found out why the class hadn't been too excited about going. They didn't think I would go in to the place when I saw it. This explained why we had eaten at a rather fancy restaurant on the previous outing.

One day of the last week, the Major suggested we quit an hour early and all go over to his house for a drink. After a polite period of meditation, I agreed. I rode over with the Major; the students walked. This was my one and only chance to get inside a middle-class house. It was a one-floor [redacted] structure set on stilts, with high ceilings and corner-to

[redacted] to cover any situation. Roughly translates to "don't worry".

EO 3.3b(3)  
PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

corner windows, perfect for the hot, damp climate. The students arrived ten minutes later, each carrying a full plate of food. In  the plates were set in the middle of the table, and everyone ate directly from them. Roast peanuts, fresh sliced mangoes and sweet sauce, roast chicken, chicken in hot sauce, fried rice and a local dish consisting of chopped by-products and pepper was the hottest food I had ever eaten. One bite and my whole head began to sweat profusely as I gasped for air. This act turned out to be as funny as my age. They all showed me it wasn't hot by eating a heaping forkful. Not one to give in easily, I had another heaping forkful. Unfortunately, the results were the same as the first time. If I had to choose one incident as the highlight of the trip it would be this hour and a half informal gathering, one of those rare times when our many differences were all set aside.

There were other moments: two farewell dinners with my first cold dish of chopped onion and chicken feet (only the pads), 100-year eggs, shark fin soup, raw octopus, squid and eel, and numerous other delicacies I can't even remember and an emotional farewell scene with my students and interpreter.

All in all, they were the hardest working, most dedicated students I've ever had the pleasure of teaching. My trip was a rich experience with six new friends I'll remember for the rest of my life.

\*\*\*\*

師  
生  
相  
好

"Nothing  
would be done at all  
if a man waited  
till he could do it  
so well that no one  
could find fault  
with it."

--Anonymous

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

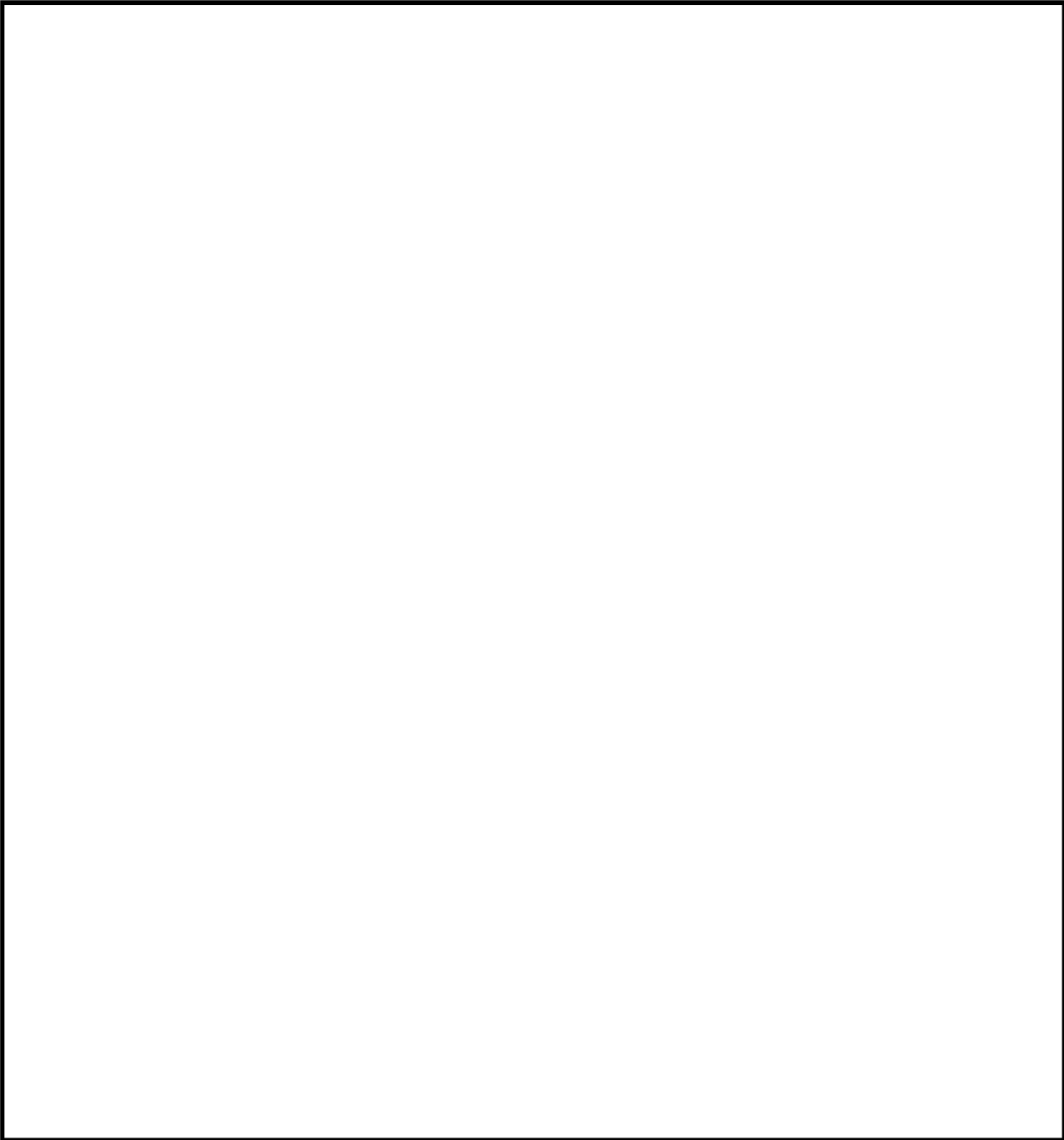
EO 3.3b(3)  
PL 86-36/50 USC 3605

SURVEYING

[Redacted]

CRYPTOSYSTEMS

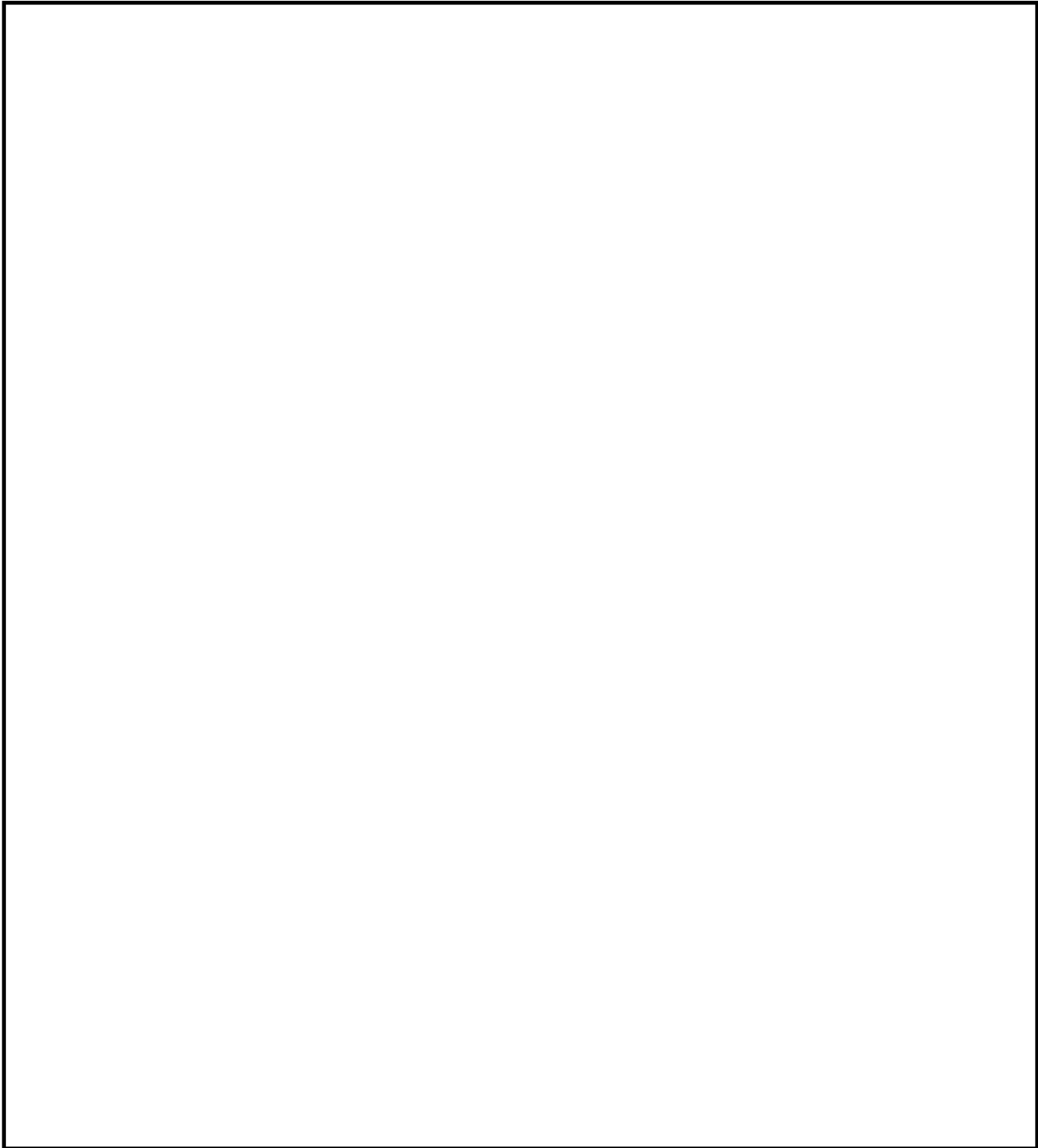
by Sam Coury, B65



~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~

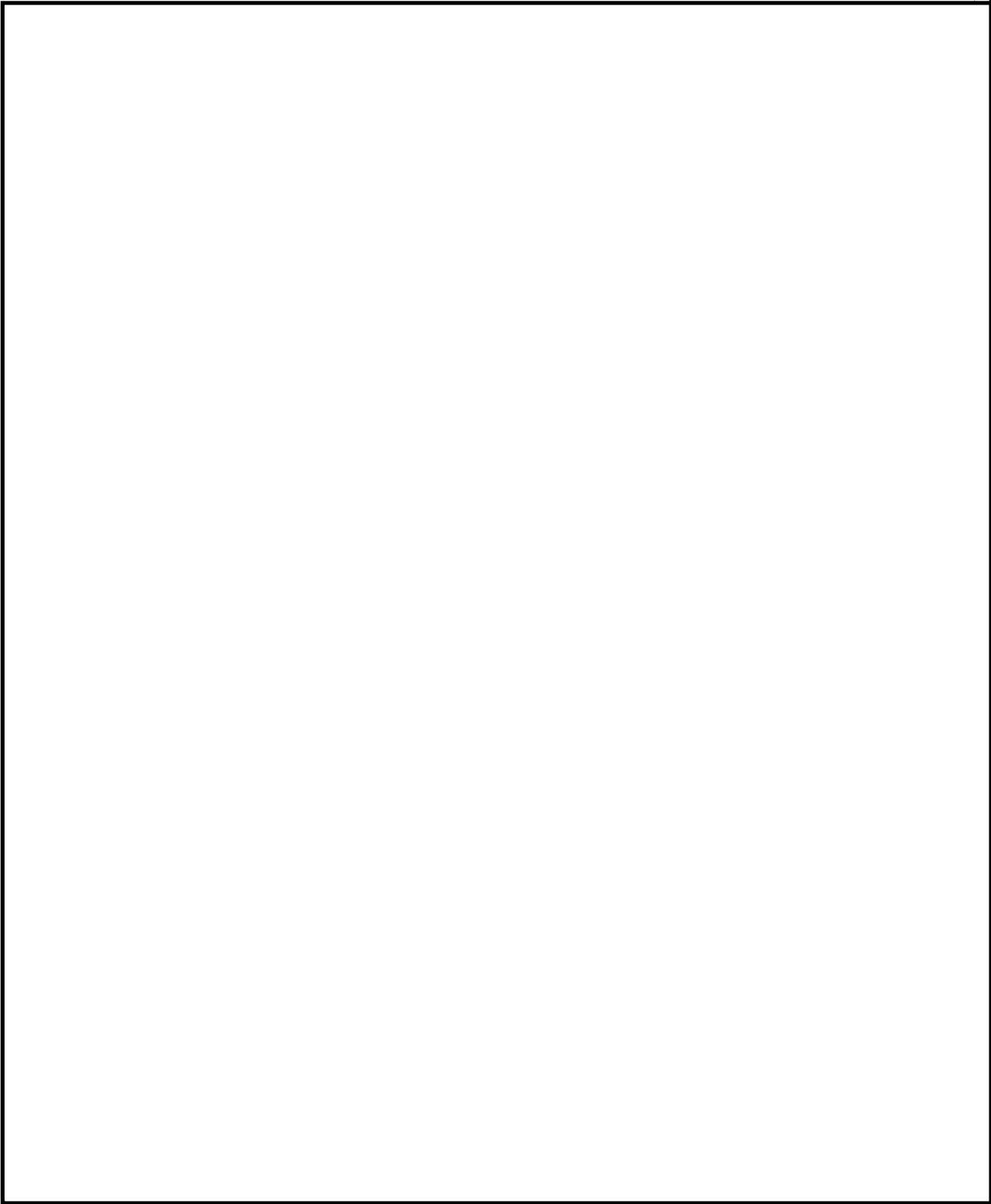


~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

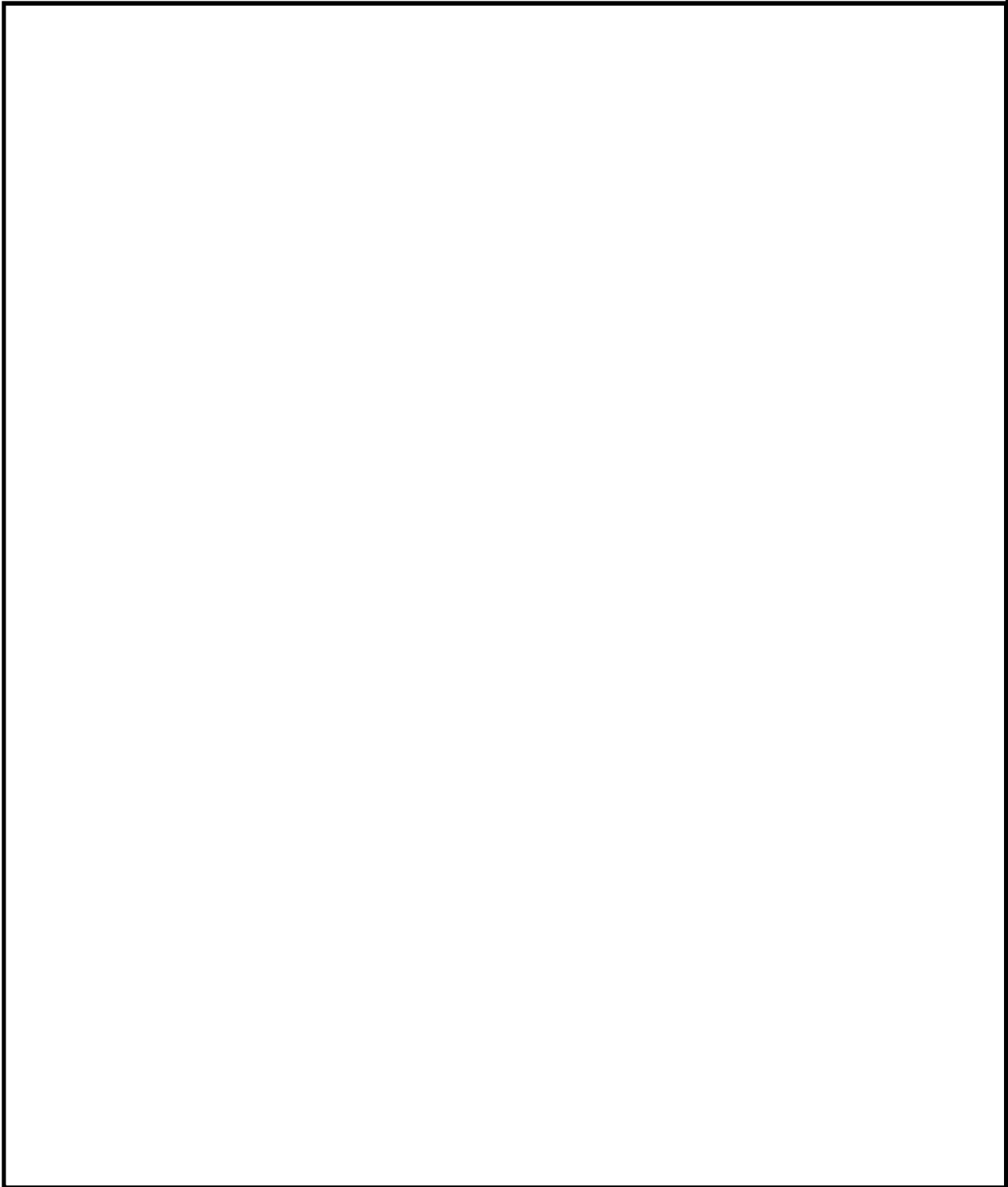
EO 3.3b(3)  
PL 86-36/50 USC 3605



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605



\*\*\*\*



*"Truly, a cart is more than the sum of its parts.*

*Better to rumble like rocks  
Than to tinkle like jade."*

--Lao Tzu

~~TOP SECRET UMBRA~~

at 1 June 65

~~TOP SECRET UMBRA~~

HISTORY OF A DRAGON

by Don DeLong, B43

According to a popular legend rooted in Greek mythology, the fire-breathing green dragon was a familiar figure and a formidable foe. During the recent fierce armed conflict in Southeast Asia (SEA), a more domesticated *purple* dragon played an entirely different role in helping to overcome the forces of evil.

Before recording the birth of the *Purple Dragon*, a slight pause for a definition of Operations Security (OPSEC). OPSEC is formally defined as: "Those actions that are necessary and appropriate to deny the enemy information concerning planned, ongoing and completed operations. This includes planning, training, and other across-the-staff procedures necessary to protect the security of operations as well as conducting OPSEC surveys to validate or improve the effectiveness of OPSEC measures." In simpler terms, it is maintaining the element of surprise, while at the same time denying information about operations to the enemy.

OPSEC, as we know it today, originated in the latter part of 1966. At that time, President Johnson expressed concern over the losses sustained by U.S. air operations in Southeast Asia and the lack of overall effectiveness.

The Director, NSA (DIRNSA), briefed the President's Foreign Advisory Board on SIGINT indications that the Viet Cong, North Vietnamese and Chinese Communists frequently had advance knowledge of U.S. operations in SEA. In the light of this SIGINT evidence, Joint Chiefs of Staff (JCS), in the fall of 1966, tasked Commander-in-Chief, Pacific (CINCPAC) to investigate the security posture of U.S. air operations in Southeast Asia. Survey teams were first organized by CINCPAC in October, 1966. Each team contained representatives from operations, communications, COMSEC, intelligence, and other sections as needed. The entire OPSEC program in CINCPAC is known as *Purple Dragon*.

Initial areas of concern for *Purple Dragon* teams, who uncovered many U.S./Allied vulnerabilities, included but were not limited to: stereotyped operating procedures; excessive plaintext voice communications; static callsigns and frequencies; physical and personnel security.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Among the first operational areas surveyed by *Purple Dragon* teams in 1966 and 1967 were B-52 ARC LIGHT strikes, ROLLING THUNDER tactical airstrikes over North Vietnam, and photo drones. In later years, OPSEC surveys were expanded to include carrier operations, gunship missions in the STEEL TIGER and BARREL ROLL areas, GIANT SCALE reconnaissance missions, Airborne Direction Finding (ARDF), Forward Air Controllers (FACs), GIANT NAIL reconnaissance missions, military operations in Korea, and numerous other areas.

In compliance with JCS memorandum SM 469-71, CINCPAC prepares a semiannual OPSEC report covering all surveys for the preceding six months. Portions of the report contain codeword material. The requirement that CINCPAC provide a semiannual OPSEC briefing to JCS and to key personnel at NSA has been discontinued.

The latest *Purple Dragon* OPSEC report in December 1972 contained findings on surveys that examined the amphibious exercise, GOLDEN DRAGON; U.S. Air Force gunships; ARC LIGHT missions into North Vietnam; Naval gunfire support; and U.S. Special Forces in Thailand.

Let us take a closer look at one of these surveys. Gunship operations, using AC-119 aircraft based at Danang, Vietnam, and Nakhom Phanom, Thailand, were surveyed in March of 1972 with augmentation of the survey team from 7th Air Force personnel and concurrent monitoring performed by Pacific Security Region personnel. Revealed were many areas vulnerable to exploitation by the enemy, which yielded valid prior knowledge or forewarning. Among the observations made by the survey was the report by gunship crews that the enemy gunners hold their fire until gunship escorts report minimum fuel (codeword BINGO) or expenditure of all ordnance (codeword WINCHESTER). This confirms that the enemy intercepts and exploits air-to-air communications to his advantage.

A number of major findings dealing with operational procedures, communications patterns, and Human Resource Intelligence (HUMINT) vulnerabilities were uncovered during the survey. Specific highlights included: (1) Use of distinctive static callsigns enables the enemy to identify, mission-by-mission, the **gunship type**, working altitude, general working area and capabilities. (2) Reporting of an escort aircraft delay, alert or cancellation by mission number via in-the-clear communications can reveal an increased vulnerability of a

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

specific gunship mission, particularly if there is no spare or substitute available. (3) DELTA and BETA points (used to identify specific geographic locations) are employed widely in insecure communications to pass sensitive intelligence. (4) Aircraft status boards display a complete and up-to-date status information relative to sensory equipment. This data could be exploited through HUMINT, since numerous foreign nationals were observed in the area. (5) Nightly gunship schedules, together with any variations therein, can be readily recovered from the unclassified operating schedule and flying schedule forms. (6) Static mission numbers, which can be readily associated with specific visual reconnaissance sectors and times on-station are a source in unprotected communications that the enemy may exploit to get advance information on any changes in the nightly gunship schedule.

Meanwhile, the OPSEC effort generated considerable interest at NSA. The responsibility to provide SIGINT support to CINCPAC was vested in a B Joint Task Force which was established currently as an NSA counterpart to the CINCPAC *Purple Dragon* effort. B45 was designated to chair the project and all SIGINT support to the OPSEC effort at CINCPAC was directed from that office.

In support of B responsibilities to provide SIGINT support to CINCPAC OPSEC, all elements were requested to be especially watchful for any SIGINT information possibly indicating enemy foreknowledge or forewarning of U.S. or Allied operations contained in enemy communications between any of B targets. It was stressed that the words foreknowledge or forewarning need not appear in the title to make the information a valid OPSEC item.

Two additional requirements were levied on B elements in support of the task force. First, all collateral and SIGINT that could possibly relate to OPSEC was to be provided to B45 on a regular basis. Also, all offices were to coordinate with B45 on all outgoing messages that pertained in any way to the general problem of enemy awareness or foreknowledge.

During its heyday in 1971 and through January 1972, the task force provided SIGINT support to the *Purple Dragon* OPSEC effort in the form of a monthly end product known as The Awareness Report, Pacific Area. Subjects of interest that contained possible foreknowledge and that were outlined in this report included: air activity, ground forces, naval activity, movement

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

of VIPS, and enemy COMSEC efforts. More specific examples within the air activity were B-52 strikes, tactical air strikes from carriers, SR-71 overflights, U-2 reconnaissance missions, and BUFFALO HUNTER photo drones.

The Enemy Awareness Report, Pacific Area, was discontinued after the January 1972 issue because a great deal of its usefulness was lost as many of the same items were reported through a more timely medium. The only current report generated by the OPSEC portion of B is a weekly electrical message forwarded only during those weeks when there is a positive foreknowledge message concerning B-52 strikes.

Although the war in Southeast Asia is supposedly coming to a close, OPSEC continues to play a vital role in support of U.S. and Allied operations in that area and in other areas of the world. To this end the office of the JCS, in July 1972, began placing renewed emphasis on their OPSEC policy guidance to the military services and the commanders of unified and specified commands.

The *Purple Dragon* remains today as a protector of the OPSEC domain. He stands ready to breath fire on those who would violate the rules of good OPSEC order.

\*\*\*\*

**CHINA DENOUNCES** another perfidious Taiwanese trick. The Nationalists, it seems, have distributed 100,000 copies of Jonathan Livingston Seagull to their people. As the Communists see it, the high but selfish ideals advocated by the best-selling novel will distract Taiwan's youth "from the just struggle for unification" with the mainland.

WALL ST. JOURNAL  
24 May 1973

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

---A complete collection of papers covering past activities of the P1 Bookbreakers' Forum on Machine Aids has just been published by P1. This document, P1 Informal No. 6, S-209,237, contains minutes of all general meetings (including two sessions for which minutes have not been issued previously), as well as a quantity of historical and background information. It should be of interest to anyone seriously involved in bookbreaking, machine support to bookbreakers, or the management of bookbreaking problems. Anyone who would like a copy should contact M.E. D'Imperio or Jean Oliver, P16, x3045.

\*\*\*\*

---RYE Project TREES is a set of 14 bookbreaking and code message processing programs that provide a fairly timely and flexible working aid for bookbreakers. TREES enables analysts to do the initial data processing and certain diagnostic tests on codes through remote RYE terminals, provides a remote access repository for data which is alterable according to the users' requirements and allows rapid data retrieval or data

The following changes to programs listed in the Project TREES manual, dated March 1971, were generated by B users:

ASH (Page A-1) - The GR (Group Size) option data parameter should be used with paper tape input, as well as card input, on an initial ASH run with the CR option parameter. ASH will insert the GR (Group Size) submitted into word 3 of the sector 1 message file identification block for use by other Project TREES programs where the group size is a factor.

BEECH (Page B-1) - BEECH will index up to 5000 records. A version of BEECH, cataloged on RYE as BEECHLG, will index up to 10,000 records. If a user wants to selectively send messages from his message file to BEECH or BEECHLG using program SPRUCE, he may do so by using standard SPRUCE program and data parameters and substituting an XX for BI as the first BEECH or BEECHLG parameter (e.g., XX90 vice BI90, if F90 is your message file).

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

DOGWOOD (Page D-2) - Another parameter to DOGWOOD, NOINC, is now available which will inhibit the automatic update of the frequency field of every code group appearing in a message submitted for a DOGWOOD decode.

FIR (Page F-1) - A user may input any size short identification, not necessarily a multiple of 5, and FIR will delete all messages with headers that match the header stream(s) submitted for the specified number of characters.

To get a copy of the Project TREES manual or to secure RYE FASTRAND storage for a Project TREES application, contact your division's machine applications representative (e.g., B42, G46, etc.). B65 has had extensive user experience with Project TREES over the last several years on a variety of [redacted]

[redacted] language) codes and can be contacted (7210s) for user-oriented assistance in establishing a Project TREES application.

\*\*\*\*



---Did you know that the Guangming Daily, a PRC newspaper, has been carrying a special feature called "Language Reform Semimonthly." The articles deal with the movement for simplifying Chinese characters and the attempt on the part of the PRC to reduce the total number of characters now being used. As of 10 May, this feature, a full page spread, has appeared on the 10th and 25th of each month.

\*\*\*\*

---The CLA Program Committee has developed what it considers to be an exceptionally informative, interesting, and stimulating lecture series for the 1973-74 year. Following is the tentative schedule:

16 Oct 73, NSA Auditorium  
THE UNITED STATES INTELLIGENCE EFFORT AND THE LINGUIST  
Dr. Louis W. Tordella,  
D/DIR, NSA

2 Nov 73, NSA Auditorium  
THE LINGUIST AT GCHO  
[redacted]

4 Dec 73, NSA Auditorium  
THE CHANGING FACE OF CHINA:  
REFLECTIONS ON TWO RECENT VISITS TO PEKING  
Mr. Charles W. Freeman, Jr.,  
Director, People's Republic of China and Mongolian Affairs, U.S. Department of State

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

15 Jan 74, NSA Auditorium  
22 Jan 74, FANX Auditorium  
PROJECT LAYAWAY: THE NEWEST  
CONCEPT IN TRANSCRIPTION  
Mr. Charles Holt,  
D/Chief, A64

12 Feb 74, NSA Auditorium  
THE FAITHFUL ECHO: THE ROLE  
OF THE LINGUIST IN U.S.  
DIPLOMATIC NEGOTIATIONS  
Mrs. Sophia Porson,  
Senior Diplomatic Interpreter,  
U.S. Department of State

12 Mar 74, NSA Auditorium  
19 Mar 74, FANX Auditorium  
INDONESIA: ITS PEOPLE AND  
LANGUAGES  
Mr. Robert S. Johnson, G92

9 Apr 74, NSA Auditorium  
THE UNIVERSAL LINK: LANGUAGES  
AND LINGUISTS AT THE UNITED  
NATIONS  
Dr. Margarita Bowen,  
Georgetown University

14 May 74, NSA Auditorium  
21 May 74, FANX Auditorium  
THE LETHAL TRIANGLE: THE STUDENT,  
THE SCHOOL, AND THE SUPERVISOR  
Mr. Alan French, E1

11 June 74  
THE ARAB WORLD TODAY  
Speaker to be announced

---New or renewing members  
of CLA may pay their 1974  
dues (\$3.00) to any one  
of the following persons:

Gallagher, Mr. Philip J.,  
B652, Room A2548, FANX II,  
ext. 7206s.

Kreinheder, Mr. Robert F.,  
B65, Room A2548, FANX II,  
ext. 7210s.

Mollick, Mr. John J.,  
B372, Room 3C099-2, OPS-1,  
FGGM, ext. 4175s.

Wagner, Miss Florence E.,  
B652, Room A2548, FANX II,  
ext. 7128s.

Wong, Mr. Washington,  
B442, Room 3W030, OPS-1,  
FGGM, ext. 4058s.

Wood, Mr. Geoffrey C.,  
B653, Room A2548, FANX II,  
ext. 7206s.

\*\*\*\*

\*\*\*\*



~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605



ASK  
THE  
DRAGON  
LADY.

THE C PARALLELOGRAM

Dear Dragon Lady:

The only thing wrong with Ms. Kennard's premise is that it does not reflect SIGINT of 1958-62 when we were reading the [redacted] [redacted] comms which told us tons about CRC. Ms Kennard should see the translations and reports put out circa 1961-62 derived from [redacted] system. I believe the reports and translations were in the VHI (later VNG) series. Several messages from CRC were decrypted and published.

My impression is that the CRC remained a viable force through the mid-sixties but began to fade as the clandestine flavor of the war died. It hasn't been heard of for years.

Finally, Ms. Kennard may well have stumbled on to the truth, but I am inclined to doubt it without more proof. Her article remains an excellent *explanation* of what might have happened. But, there have been several de facto reorganizations within the Communist hierarchy since the mid-sixties and I suspect that the CRC, if it still exists, is a paper organization.

Tom Glenn, B61

Dear Dragon Lady:

Ms. Kennard's article on the "C" parallelogram in the June issue of "Dragon Seeds" provides the opportunity to expound on the problems encountered in the use of collateral information in the war in South Vietnam.

As she states, the war has produced (and is still producing) a volume of collateral that has probably never before been available to our analysts. This very volume, however, often proves to

~~TOP SECRET UMBRA~~

be a mixed blessing. To paraphrase Newton, "for every piece of supporting collateral there is an equal and opposite piece detracting." It has been postulated that given any conceivable premise, no matter how obtuse, collateral can be found which will provide substantiation. Although this statement is obviously uttered with tongue in cheek, it is nonetheless true that often it is the traffic analyst that must bail out the info analyst and not the converse as Ms. Kennard has suggested.

In her study, Ms. Kennard cites an ARVN J2 study based on captured documents but fails to mention that the documents also positively indicated that the ubiquitous Agency "C" has both a sapper and signal command. Messages from VC MR 3 specialized agencies (such as sapper and signal) were addressed to the "Sapper Command of C" or "Signal Command of C." C also sent messages to VC MR 3 asking for information and demanding that it forward reports on enemy military activity including after action reports. Is it not unusual that the CRC, equated to "C" by Ms. Kennard, "has no communications of its own" yet has its own signal command?

Further, the document which lists the No. 2 man of the Cau Ca (CRC) as the political officer of "C" is inconclusive in the equation of C to CRC. It is known that high ranking party members, not only of the central party headquarters in North Vietnam (aka C (?)) but also of COSVN (aka R) in South Vietnam, "wear two hats" and function on several committees. Could not the political officer of "C" also concurrently be the No. 3 (?) man of the Cau Vu resulting in yet another "equation."

Once again the study of collateral information has proven to be an esoteric discipline and has allowed different analysts to proceed along different paths each seeking that piece of information which will support a hypothesis formulated from analysis of previous data.

Thomas Lahr, B62

\* \* \* \*

*Continuing the discussion on the plight of the Agency's linguist, the Dragon Lady shares these thoughts from a senior linguist:*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

"A PROGRAM FOR THE IMPROVEMENT OF THE LANGUAGE CAREER FIELD"

1. Set up a scale which distinguishes more clearly between the plodding, factory-hand linguists and the expert, innovative and intelligence-minded ones. At present I suspect they are all lumped together in the mind of management, and this accounts for the low estate of language as a calling.
2. Make language professionalization tests rigorous enough to discriminate not only between well-qualified and poorly-qualified linguists but also between professional linguists and dilettantes from other fields who just think they'd like to pick up another certificate on the cheap.
3. Recognize some of the newer fields of language work: comprehensive language files, computerized language aids, computer analysis of plain language phenomena, effective aptitude and achievement tests, and even "blue-sky" projects like linguistic approaches to encoded voice and ways of solving the transcription problem.
4. Publicize achievements in the language field -- both among managers and among other linguists.
5. Promote linguists for linguistic work, that their days may be long in their own field and that the newer generation may be inspired to enter that field and to give it their best and their all.

*Recognize - Publicize - Promote!"*

\* \* \* \*

"*ໂຕ ຜີ ຈຸດ ຈຸດ ຈຸດ ຈຸດ*"

*"The foot of an elephant closes the  
mouth of a chicken."*

--Laotian proverb

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

SOLUTION TO JUNE 1973 TRANSPOSITION PROBLEM

FOUR SAGES AND THEIR SAYINGS  
7 15 23 16 18 1 8 5 19 2 13 4 22 10 6 11 17 20 3 24 12 14 9 21

THE SAGES OF CHINA AND THEIR RECORDED SAYINGS REMAIN TO THIS HOUR MIGHTY FORCES IN THE LIFE OF THE WORLD XX THE GEMS OF WISDOMS OBVIOUSLY IN THEIR CLEAN CUT DIRECTNESS HAVE HAD INFLUENCE FAR BEYOND THE CONFINES OF CHINA AND THE ORIENT XX THEY GLOW IN THE LITERATURE OF ALL LANDS MODIFIED XX AND PERHAPS A LITTLE DISTORTED AT TIMES XX INFORM AS THE CENTURIES PASSED AND APPLIED TO CONDITIONS PARAMOUNT IN THE TIME OF MANY AUTHORS WHOSE WORKS CONSTITUTE THE BACKGROUND OF LIFE IN VARIOUS COUNTRIES XX WITH THE PASSING OF THE YEARS THOSE GEMS HAVE BEEN CALLED UPON TO SERVE DIVERGENT PU

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

R P O S E S I N N U M E R O U S I S M S X I D E  
O L O G I E S X A N D S O C I A L A N D E V E N  
R E L I G I O U S F O R M S X X T H E Y F L A S  
H A T O N E F R O M U N E X P E C T E D P L A C  
E S I N M A N Y O F T H E S T A T E L Y L E A T  
H E R B O U N D T O M E S O F T I M E S A L R E  
A D Y C O N S I D E R E D O L D E N A N D I N M  
O R E M O D E R N W O R K S A L S O X T H E L A  
T T E R I N M O S T C A S E S H A V I N G S E T  
T H E M F I R M L Y B E H I N D B A R S O F C O  
P Y R I G H T X X W E K N O W T H A T T H E S A  
G E S W O U L D N O T M I N D S O L O N G A S K  
N O W L E D G E A N D W I S D O M C O N T I N U  
E T O S P R E A D T O A L L H U M A N I T Y X Z

Encipherment involved transcribing by key column in an alternate vertical route.

\* \* \*

SOLUTION TO CRYPTO-SCRAMBLE:

1. Generatrices
2. Tempest
3. Relative Base
4. Shadow
5. Superstet

CRYPTOSANSWER: REPEAT RATE

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
EO 3.3b(6)  
PL 86-36/50 USC 3605

## CONTRIBUTORS

RICH ATKINSON, E13, is a graduate of the University of Colorado who joined NSA in 1963 and was immediately assigned to P1 where he has spent most of his Agency life. He has accomplished a 3-year tour in Cheltenham, England and the P1 Crypto-Math Intern Program (not necessarily in that order) and is recognized as a professional in the fields of Mathematics, Cryptanalysis, and Education and Training. Rich can currently be found at the National Cryptologic School using baseball batting averages to illustrate the theory of probabilities for budding cryptanalysts (and wondering how we got this sketch).

SAM J. COURV, B65, began work for NSA in 1948, spent nine years as an analyst of [REDACTED] cryptosystems. Subsequently, from 1960 to 1962, he served a tour of duty in Cheltenham, England where he was concerned with [REDACTED]. Immediately afterwards, he joined B Group and was tasked with analyzing first VC and then Southeast Asian diplomatic cryptosystems. Since 1966, he has been responsible primarily for cryptanalytic efforts against [REDACTED] cryptosystems.

CAPT DON DELONG has spent the last two years of a 12-year Air Force career working in the OPSEC portion of B45. He holds a degree in Business Administration from Southwestern State College in his native Oklahoma. A former Morse intercept operator, Capt Delong lists among his military assignments such widely scattered areas as Alaska, Germany, and Thailand. While in Southeast Asia, he provided SIGINT support to ARC LIGHT missions and maintained a secure communications facility in support of BUFFALO HUNTER photo drone missions and GIANT NAIL (U-2) reconnaissance overflights.

JANE (BETTY) DUNN's connection with SIGINT dates back to WWII and covers targets from Japanese Military to CHICOM [REDACTED] with stops along the way for work on [REDACTED] European Satellite, and Vietnamese Communist cryptosystems. She holds a B.E. from Duquesne University and was prepared to teach French in Pennsylvania high schools before she was detoured to Arlington Hall. Betty is a certified cryptanalyst, a tutor for the CA Intern program, an E.E.O. counsellor, and the biographic editor for DRAGON SEEDS. Chief of B45, the PRC [REDACTED] Division, from May 1972 until the reorganization of July 1973, Betty is now a member of the B4 Technical Directorate for Cryptanalysis.

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

JERYL O. (JERRY) GEGAN, B652, joined NSA in 1966, following a stint in the Army Security Agency. He has worked as a linguist, reporter, and traffic analyst in both the [redacted] sections. In 1968 and again in 1971, Jerry served as a Lao linguist on temporary loan to a [redacted] field site. From 1969 to 1972, he was the B12 integrated analyst for Laos at USM-7 (Udon, Thailand). Jerry is Chief of the [redacted] Chairman of the Lao PQE Committee, and certified by both the Language and Special Research Career Panels.

機

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

保  
密



it's classified!!

~~TOP SECRET UMBRA~~

~~TOP SECRET~~

# National Security Agency

Fort George G. Meade, Maryland



DECEMBER 1973

# DRAGON SEEDS



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~TOP SECRET UMBRA~~

This is *Dragon Seeds*.

There is fantasy, irony, and the bite of reality in the name. It speaks of the East. And, like the East, it suggests much, says little.

*Dragon Seeds* is both Mother China and her neighbors. *Dragon Seeds* is monumental and minuscule. It is the past and future. It begs for elaboration but gives none. In it are echoed softly slurred Mandarin, brittle Vietnamese, determined Korean. In it is the spectre looming over the Thai, Lao, and Khmer. It is frightening and friendly. It is uncertain.

Above all, *Dragon Seeds* is promise. It is fertile with ideas unbounded, to be cultivated with creativity and imagination. It is challenge. It is alive. It will be more than it is.

*Dragon Seeds* is yours. May it grow with you.

The Editors

~~TOP SECRET UMBRA~~

DRAGON SEEDS

Publisher

DONALD E. MCCOWN, CHIEF B4

Managing Editor  
Minnie M. Kenny

Executive Editor  
Robert S. Benjamin

Rewrite Editor  
Jane E. Dunn

Special Interest Editor  
Ray F. Lynch

Feature Editor  
Robert F. Kreinheder

Education Editor  
Marian I. Reed

Composition

Louella M. Ertter

PRESS CORPS

- |     |                     |     |                      |
|-----|---------------------|-----|----------------------|
| B11 | Carolyn Y. Brown    | B42 | Peggy Barnhill       |
| B2  | George S. Patterson | B43 | Mary Ann Laslo       |
| B31 | Jack Spencer        | B61 | <input type="text"/> |
| B32 | Jean Gilligan       | B62 | Edmund J. Guest      |
| B33 | Louis Ambrosia      | B63 | William Eley         |
| B41 | James W. Schmidt    | B65 | Philip J. Gallagher  |

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605



VOL 2  
NR. IV

DECEMBER 1973

**TABLE OF CONTENTS**

Chinese Communications Developments..... Jack L. Thomas 2

1972-73: A Viet Nam Odyssey...Leo Stepp & Edward O'Connor 8

Christmas at the School..... Morris L. Ferguson 17

Time to Look at People..... Tom Glenn III 19

The Open Door: Are You Using Computers?...Dr. Walter Jacobs 21

Minnie's MINI..... Minnie M. Kenny 23

B Needs Its Own Computer..... William P. Stivers 24

[Redacted Box] Russ Myers 31

Seedlings

Ask the Dragon Lady

Contributors

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

*With this issue, DRAGON SEEDS marks its second anniversary. I am pleased, on behalf of all of B Group, to extend to its publisher, editors, press corps, and contributors congratulations and thanks for making it a successful and useful publication. We have all benefitted from your efforts.*

**DRAGON SEEDS**  
*has demonstrated its worth as a valuable means of exchanging information among people in B. For analysts and technicians, it has provided an outlet -- a means to share ideas, to tell others of successes, to learn about new or different techniques, to express concerns, and to ask questions.*

*For others, it has given a new understanding of operational problems, highlighted additional areas of interests and offered some new perceptions on how we go about our business. It has made us aware of important developments not otherwise publicized. For all of us, DRAGON SEEDS is informative; it invites us to think; it helps us to do our jobs better.*

*We all should work to see that DRAGON SEEDS continues to serve us well. With our continued interested support and willingness to contribute articles, it will remain a relevant and useful way to share operational and technical ideas within B Group.*

**Happy anniversary, DRAGON SEEDS!**  
*May you continue to instruct, inspire, and provoke us.*

*Wm C. Jackson*

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~CHINESE COMMUNICATIONS DEVELOPMENTS (Where Have They Been,  
Where Are They Going?) by Jack L. Thomas, B44

*There is high technology in China today. Indeed, it would be fair to speak of an electronic revolution in many fields.\**

This statement will undoubtedly raise eyebrows of a number of readers and trigger the response: which China are we talking about? Certainly not the People's Republic of China? But we are talking about the PRC. And the statement for the most part coincides with beliefs held by the handful of Chinese "technique watchers" who have followed evolving PRC communications developments and trends throughout the years.

But how did the Chinese reach this point so suddenly, apparently without our knowing about it until only recently? The answer is that they, of course, did not reach this point suddenly, nor recently. It has been evolving over a number of years, and generally speaking, we have been aware of it. What the Chinese have denied us over the years has been the detail needed to tie the bits and pieces into an overall China-wide picture. Their penchant for security, bordering on national paranoia, is well known to analysts who have followed the problem from any standpoint throughout the years, and this pertains to the communications technique watchers as well.

This is not to say, though, that these analysts were totally blind to the overall picture that was evolving, nor were they totally without information to predict specific developments which later often proved highly accurate. Documentation exists that will substantiate accurate reporting on developments and trends in many areas of the Chinese communications establishment. These predictions, however, were of necessity frequently general, having as their basis a variety of sources which were often too anemic, too sparse, or too tenuous to permit their being pieced together into a picture showing precisely what the Chinese were doing, or where they were headed. Nor in many cases were they sufficient to permit detailed statements of specific PRC communications developments and trends that could be defended to the degree necessary to justify planning and programming actions.

*\*From "High Technology in China," Scientific American, December 1972, by Dr. Raphael Tsu, an IBM physicist who extensively toured Chinese factories, universities, and research centers in the summer of 1971. (See the Summer 1973 issue of the Cryptologic Spectrum for a review of this article.)*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Though in many instances analysts watching the problem daily could sense probable future developments, they were often hard-pressed to document their beliefs. These analysts were of necessity a cautious group. They had to be, given the paucity and shakiness of their sources, the scope of the problem confronting them, and the rareness of their species.

In addition to their strict adherence to security, the Chinese further frustrated analysts throughout the years by displaying amazing talent for being unpredictable. They would surge forward in certain areas, apparently determined to pursue these avenues to satisfactory conclusions. But as analysts began to predict future trends on the basis of these developments, the Chinese frequently (and often without apparent reason) changed their course, or in some instances stopped development of a particular technique or system and showed no apparent future interest in it. Especially perplexing was the fact that some of these efforts afforded the Chinese distinct advantages, far outweighing other courses of action, and in many cases seemed ideally suited to their particular needs. Nor did they always develop their communications along lines considered advantageous by Western standards, though in many areas the technology involved was almost certainly available to them. But we should also keep in mind that what seems to us to be aberrations in Chinese developments, may stem from either a lack of consensus among their planners on long-range goals, or our inability to share their perspective on long-range goals.

This is not to say, however, that Chinese communications developments were stagnated during the years, or showed no sustained advances. Far from it. The PRC has long considered communications and electronics to be high on its national priorities list. Consequently, internal disturbances such as the Cultural Revolution apparently did not slow research and development significantly in this area, as was also apparently true of other high-priority areas. And when the situation the Chinese inherited in 1949 is additionally considered--amounting to an almost non-existent communications capability decimated by years of war and few factories capable of producing needed equipment and systems--they have done quite well indeed. This is all the more noteworthy when one also considers the almost total cutoff of Soviet technical aid to China in 1960, and, until recently, difficulties the Chinese encountered in obtaining technology, equipment, and systems from the West because of trade embargoes and restrictions.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Discussing how to improve their motors.



Workers of the Electric Appliances Repair Shop have made this equipment to produce silicon elements.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

At the same time, however, the Chinese have not totally been without Western help, nor did the Sino-Soviet rift totally stop their progress. By 1960 the Soviets had given them a solid base upon which to expand--from components, equipment, systems, and technology to whole factories. This Soviet assistance, coupled with the considerable quantities and varieties of equipment and technology not subject to Western embargo, enabled the Chinese to leap perhaps as much as 10 to 15 years ahead of what otherwise probably would have been the case. Additionally, the Chinese learned a valuable lesson from the Sino-Soviet rift and from the difficulties of acquiring assistance from the West. From about 1960 they increasingly turned, of necessity, toward self-reliance in this and other highly technical fields.

But much of the equipment and technology gleaned from the West was not the most sophisticated, by world standards, at the time they acquired it, and it was by and large limited to components and specific equipments. Large and complete systems and the factories to build communications items were almost totally denied the Chinese by trade restrictions. But the technical aid the Chinese did receive nevertheless represented significant steps forward for them and gave them technology and equipment that could be copied, produced, adapted to their particular needs, and used operationally--and in some cases, later improved upon as well. Foreign equipment and technology afforded them the sorely needed base upon which to build their communications establishment--through copy, modification, and domestic manufacture. And although Soviet technical aid was severed in 1960, the equipment, systems, and technology acquired from the Soviets before the rift served the Chinese well for years to come.

The rest the Chinese for the most part apparently accomplished on their own, displaying along the way their well-known ability to "make-do" with what they had available, and leaving the acquisition and employment of sophisticated technology to follow in due course, after basic needs had been satisfied. Through this process, and through increasing interest in more sophisticated techniques in recent years, the Chinese have developed their communications establishment to the point where today it can be said to be capable of supporting the basic needs of the nation.

One word of caution: the Chinese may--and probably do--have technology and equipment of higher sophistication and in greater quantity than they have been given credit for. As noted previously, no target nation has in the past revealed less about its technical progress. Fortunately, however, we have been able to learn something additional about Chinese design and production from captured

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

equipment in South Vietnam, some of which Agency engineers compared favorably with the latest Western technology in this area. But surprising as this was, even more disturbing was the fact that certain of these equipments had been available to the Chinese military in considerable quantities years before they were captured, and that we had no previous information whatsoever about them. Their existence was a total surprise, and so was their degree of sophistication. Nor are these probably isolated examples; there is little doubt that the Chinese have developed tactical--and other--equipment and systems incorporating high-quality design about which we are unaware, and about which we may not become aware except in contingency operations or a national emergency.

Having developed a communications system capable of supporting the basic present-day needs of the country, where are the Chinese headed in the future?

The recent and dramatic rapprochement with the U.S. and other Western nations, coupled with Chinese determination to advance rapidly as an industrial power, will call for sharp increases in both the quantity and quality of communications facilities--both internal and external, both radio and landline. At the same time, slackening of trade restrictions will make advanced Western technology, equipment, and systems increasingly available to the Chinese. And they seem determined to avail themselves of them to quickly bridge present gaps--not just single sets and components that they can copy and produce, but entire systems as well, and in some cases factories to produce them. They now state publicly that they are in fact after entire systems and factories to the limits their economy and foreign exchange will permit, and that they want them as fast as they can be acquired. There is little doubt that they will get them, and that the Chinese will insist on, and will receive, varieties incorporating the latest technology.

This availability of advanced Western technology and equipment, combined with their own rapidly expanding domestic design and production capabilities, point toward solid future Chinese successes in these and related areas. Also to be kept in mind: China, like other Communist countries, can concentrate tremendous effort on areas of national priority, and communications and electronics advances could therefore occur at a faster rate, and at higher levels of sophistication, than present information may indicate.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

In conclusion, the Chinese are on the threshold of an electronic revolution, and within the next decade will demonstrate technological progress that will place it among the advanced industrial powers of the world in this and other highly technical fields. Chinese communications and electronics developments in future years will, therefore, become an increasingly interesting and challenging problem to follow, steadily becoming more complex, but at the same time providing more--and more reliable--material to our analysts, thanks to the "opening up" of China. This situation will place increasing demands on those in the Intelligence Community responsible for keeping abreast of such developments, and on those at NSA, where we like to keep ahead of them.

Yuhsien County workers produce coal tar, gasoline, diesel fuel and asphalt with simple equipment they made from waste materials.



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~1972-73: A VIET NAM ODYSSEY

by Leo C. Stepp and Edward A. O'Connor, F46

*Approximately 125 kms SSW of Saigon, four hours by bus, six and one-half hours by cyclo, two tanks of gas by Honda, and forty minutes by Air America "Gooney Bird" in Phong Dinh Province, Central Mekong Delta, lies the beautiful tropical splendor of Can Tho City and sanctuary/hide-away for IV Corps' ruthless, intrepid U.S. Advisory Team.*

It was the Lunar Year of the Rat when the Odyssey began. The mission was to advise South Vietnamese Army (ARVN) personnel while they assumed the U.S. SIGINT mission in the delta from USM-607. Since there was no established precedence to follow, each problem encountered had to be dealt with in a unique manner. Realizing that extensive changes were essential to make the transfer of responsibility efficient, the first priority of the advisors was to circumvent the inherent language barrier and to establish a workable rapport with their ARVN counterparts. This was achieved, to some extent, through patient guidance and constant interface, i.e., sign language, graphic illustrations, etc. With such techniques at their disposal, advisors began to examine the innumerable problem areas.

Initial corrective efforts were directed at security procedures which were almost non-existent. The following aberrations were rectified immediately: first, there was no ARVN officer on duty during weekends or holidays; second, an excess of defunct classified material was stored in file cabinets and boxes; third, and most important, ARVN personnel were not familiar with the use of the numerous incendiary devices for the emergency destruction of crypto-gear and classified documents. In addition, advisors established a picture badge identification system and access list for all authorized personnel. This list excluded one unidentified, indigenous individual who purportedly was employed by the 335th Radio Research (RR) Company to guard the antenna field.<sup>1</sup> Although the unit (335th RR Co) departed, Nguyen (???) remained vigilant as ever, at the expense of an unknown source.

Concurrent with improving security practices, a program to extend Manual Morse intercept capability was implemented. Vietnamese operators had and were continuously receiving

1. *Can Tho Centers antenna field is located in a non-secure area approximately 500 yards NE of the operations bunker.*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

training in intercept techniques, but their proficiency was far below that of their U.S. predecessors. Specifically, their copying speed was approximately eight words per minute, they could not backlink activity, and they were unaware of the effectiveness of Morse operator characteristics analysis. After discussing these problems with the ARVN commanding officer (CO), advisors received permission to reorganize and supervise the training program. The new program was successful enough, so that the supervision was eventually returned to the ARVN's. When new personnel arrived, they assumed their duties with a minimum amount of on-the-job training (OJT). However, after several months the operators, as well as other personnel, began to lose their incentive. To eliminate this negative attitude, the ARVN CO was convinced to initiate a "Soldier of the Month" award. This consisted of 5,000 Piaster (provided by the advisors) and a Letter of Recognition. By U.S. standards the award was minimal, but the ploy worked. The competitive spirit between sections increased; and following the first presentation, all personnel were striving to achieve this award.

The first award was presented to the Airborne Radio Direction Finding Ground-to-Air radio operator. Significantly, the ARDF tip-off function had undergone an extensive transformation and emerged from a state of chaos and confusion to the point of receiving special recognition. In fact, standard operating procedures were produced by this section and disseminated for employment throughout South Viet Nam.

Following the cease-fire and associated withdrawal of American military personnel, the U6A ARDF aircraft assigned to the U.S. 146th aviation company were transferred to Saigon. Although four missions were tasked from Saigon daily numerous problems occurred and approximately one mission per day was flown. Believing ARDF effectiveness could be increased with additional missions, advisors clamored for the assignment of ARDF aircraft at Can Tho Center (CTC) and the accompanying requirement for preparation of tech data lists (TDL's) for each mission. When four U6A's were finally returned to Can Tho, the ARVN's did not possess the sophisticated secure air-to-ground voice communications as American predecessors, and relied solely on the much slower process of one-time pads. Nevertheless, with Can Tho assuming control of the aircraft and providing mission tech data, ARDF results began to improve and personnel were instructed in methods of altering mission frag points to maintain greater cognizance on priority targets. As a result, more information was provided traffic analysts, enhancing development efforts.

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

In the early stages of the Vietnamization improvement and modernization (VIM) Program, there were only five analysts assigned to the T/A section; two of which were radio operators for ARDF ground-to-air tip-off. The remaining three were required to devote all their time to preparing and transmitting daily TECSUMS. To increase productivity, five additional analysts were transferred to CTC, but they had only recently completed school and were unfamiliar with operations. Complicating this situation, the new people spent almost three months painting, filling sand bags, and satisfying other administrative trivialities. When they were finally released to operations, their training was accelerated. In March 1973, the procedure for filing tech data was altered, a new system to handle unidentified entities was established, and the TECSUM format was revised to facilitate changes. Once analysts overcame their fear of error, development was successful and new entities were notated and forwarded as isolated.

Although positive results were being attained, a recurring difficulty plagued the TA section: the perplexing importance of serialization (NR's) and chatter extracts and the necessity for accurate logging of all entries to satisfy a computer -- an alien wonder they had never seen but were told existed. In addition to the lack of experience and comprehension, only one traffic analyst spoke English and he was hospitalized with pneumonia for three months during this critical period. Instruction (pointing and drawing illustrations) was provided through non-analytic interpreters and with the limited operational Vietnamese of the advisors. After many hours of frustrating and occasionally humorous guidance (on the part of both advisors and ARVN personnel), periodic checks of the TECSUM and raw traffic indicated a continued improvement and a decreasing error rate.



Similar complications occurred with exploitable message reports (EMR's) in the cryptanalysis section. Lack of experience again was a prime detriment and initially no exploitation was performed. Personnel only logged and forwarded EMR's from the three ASTD's.<sup>2</sup> Once the C/A shop was expanded to twelve analysts, a training program (basic cryptanalytic techniques) for exploitation and identification of messages was instituted. Since the ARVN's readily adapted to the program and acquired the basic skills rapidly, one man was sent TDY to each ASTD to establish similar programs of instruction. Eventually 90% of low-level voice intercept was identified, new cryptosystems were isolated and forwarded, and local commanders received required perishable intelligence.

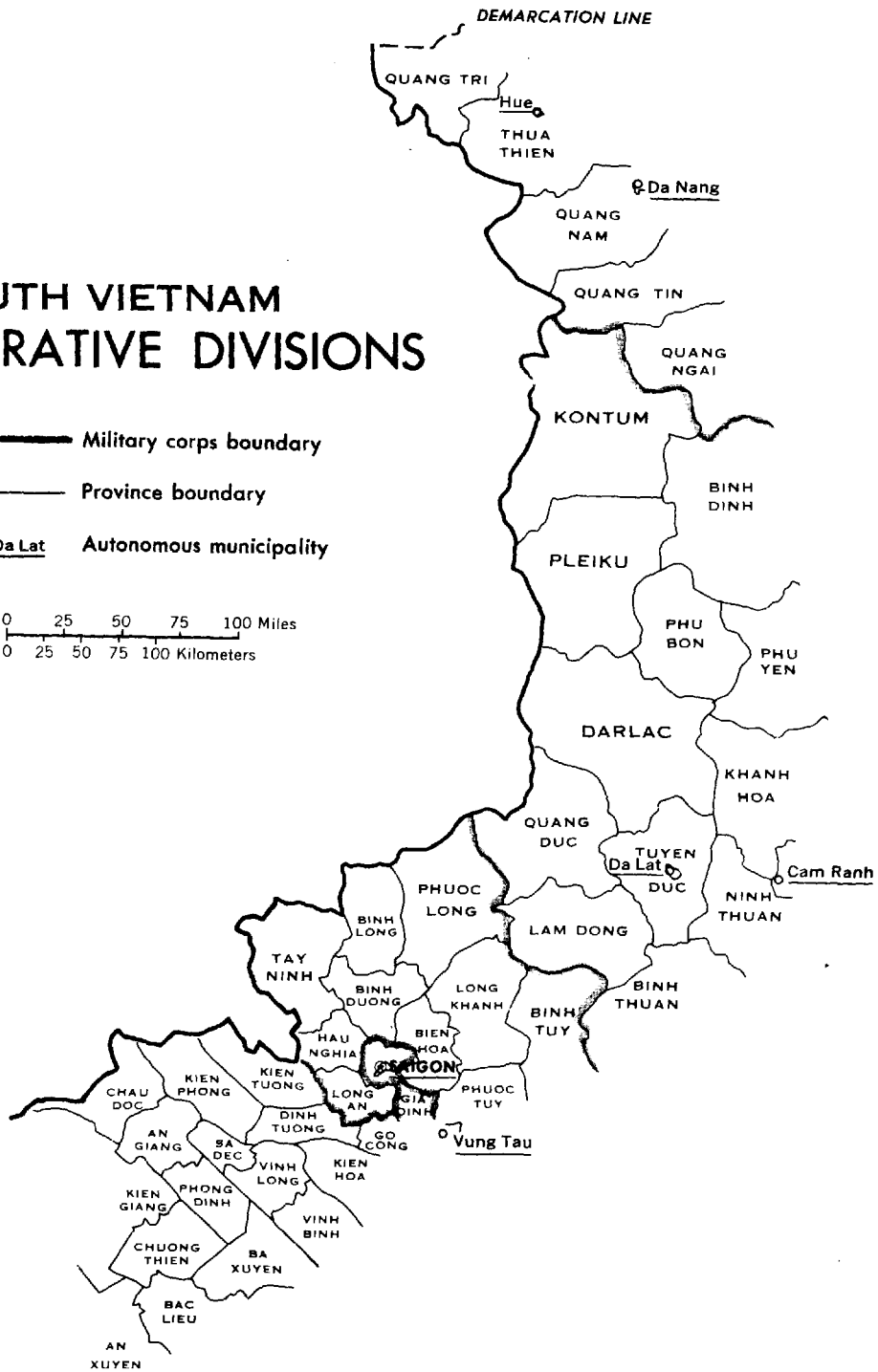
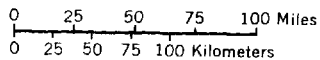
Z. ASTD expands to ARVN Special Technical detachment.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

# SOUTH VIETNAM ADMINISTRATIVE DIVISIONS

-  Military corps boundary
-  Province boundary
- Da Lat Autonomous municipality



DAO PHU QUOC (KIEN GIANG)

CON SON  
(Administered from Saigon)

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Although results were favorable, there is no implication intended that the cryptanalytic effort was without its peculiar headaches. Numerous problems were experienced in couriating intercept from LLVI teams and from ASTD's when circuit outages occurred. Since the situation vacillated in direct relationship to the tactical environment, advisors were stymied in endeavors to alleviate this dilemma. Despite the requirement, air transportation (helicopter) was seldom available and courier by road was extremely hazardous. Yet LLVI teams attempted courier every two-to-three weeks and when necessary even traveled by bus in civilian clothes. Without any secure means available to transmit intercept for preparation of EMR's, these methods were the only alternatives to satisfy demands for timeliness.

Although timeliness is an innate characteristic of the SIGINT mission, natural and man-made phenomena often alter the course of events. An excellent example was the selection of a location and construction of CTC's AN/TRD-23 medium range direction finding (MRDF) site. Between July and September each year, the tropical monsoons visit Can Tho. Again, field expediency dictates "nothing shall be wasted" (to include monsoons); therefore, concurrent with the arrival of the monsoon was Can Tho's Annual Aqua Festival". Although these festivals improved morale and helped solidify relations with the local inhabitants, the "Year of the Rat" proved to be the last of the aquacade follies. In May 1972 land surveyors from Engineer Region IV (ER-4) inspected the only possible location for Can Tho's proposed MRDF site, which unfortunately, was one and the same as "mini-lake" where the festivals were held. The surveyors estimated that approximately 7,000 cubic meters of fill dirt would be required to displace and remove all the water from "mini-lake" so that a base for the site could begin.

All of these calculations led to numerous questions (not to mention where next year's Aqua Follies would be held): "Where would this amount of dirt be found?"; "Once found, how would it be transported to the proposed site?"; and finally, "Who would finance the venture?"

Because this MRDF site would be an integral part of the ARVN MRDF net serving all of South Vietnam and would be manned by ARVN personnel, it was automatically assumed that the ARVN's would make all financial and building arrangements. After two months of ARVN procrastination, paper shuffling, and overall apparent apathy, the advisors decided to initiate some action.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

There were two weeks of rambling over the countryside in a jeep, over roads previously traveled only by reconnaissance teams. Then the advisors found a large "farm-like" residence, with an expanse of adjoining land. After several hours of verbal ping-pong, threats, shouts, obscenities, and finally handshakes, the advisors had bargained with the owner for the required amount of fill dirt. The nominal fee agreed upon was eight 55-gallon drums of gasoline (hopefully provided by Uncle Sam) and six cases of American beer (provided reluctantly by the advisors from their very limited personal cache).

The fill dirt dilemma was solved; transporting it from the farm to "mini-lake" was still another predicament. After several sociable evenings with members of the ER-4 team, the advisors were able to borrow several five-ton trucks and one front-end loader to fill them. There were no operators available to run any of the machinery, so the ruthless, intrepid advisors began a "trial and error" fill dirt operation, that would have put "Conte" out of business in a week. Anyway, two weeks and 184 truckloads later (overlooking hours of exasperation at the controls of the front-end loader, or back and vocal strain when trucks were "unprofessionally" backed too far into "mini-lake" and had to be "push-pulled" out), the base level was nearly workable. However, continuous rains along with the rising water table, postponed any substantial achievements until early December '72 when the earth finally dried up and initial work began on the installation of the TRD-23.

While operations were running as smoothly as could be expected at "mini-lake", 500 meters to the Northwest was another facet of the MRDF project. This was the location of the obsolete AN/TRD-4 site where some of the equipment for the "mini-lake" had been stored. The removal of this equipment left only the hut, connecting cables and antennas. By order of the Commander of Can Tho airfield, a different section of perimeter grass was burned each month. As fate would have it, the date for burning grass in the area of the TRD-4 site coincided with the operation at "mini-lake" and no advisors were available to monitor the burning. G.I.'s from the airfield command trudged out early one morning to begin their detail. With gasoline cans and blow torches, they began what was supposed to be a small, controlled, well supervised grass fire. All went well for the first hour or so. Personnel were strategically placed armed with shovels and rakes, just in case something should happen. An undetected slight change of wind (in velocity and direction), began to move the fire towards the AN/TRD-4 hut and its many antenna cables. Before

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

anyone realized what was happening, the highly inflammable cables began to burn and spread towards the remaining antennas. This probably could have been stopped with a minimum of effort, if there had not been a war in progress. ARVN helicopters returning from a sweep and destroy mission, flying low over the airfield, fanned the flames in every direction at once, creating pandemonium and mass chaos. Before the fire could be brought under control, approximately \$1,500.00 worth of cable, connectors and antennas had been destroyed.

Meanwhile, back at "mini-lake", to insure that future rains would not destroy the equipment installed for the TRD-23, everything was elevated 1 foot. This was accomplished by pouring concrete antenna pedestals (12" high) for each of the 26 antennas and two (12" thick) 12X18' slabs to support the generators and the TRD hut. All this was completed in three weeks, with most of the time being consumed scrounging cement and lumber for forms. Before any antennas could be placed on their respective pedestals, four perimeter poles (each 40' high) had to be erected in each of the four corners of the antenna array, with aircraft warning lights fixed to the top of each one. (This was necessary because "mini-lake"/TRD-23 site was only 200 feet from the end of the Can Tho airfield runway). As soon as the poles were in place the lights had to be operational; thus another project was temporarily halted until a power source could be found. The only generator in the area was owned by the Pacific Architects and Engineers (PA&E/-AKA- promises, alibi's and excuses); so advisors approached them and obtained permission to use their generator. Yet another delay of three weeks was incurred because PA&E had another requirement to supply power for the joint military commission (JMC) and the international commission for control and supervision (ICCS) peace-keeping forces while they were at Can Tho airfield. The delay came as a blessing. Checking their cable supply, the advisors discovered a shortage and the generator in question was approximately 1/4 of a mile away. After securing additional cable, the day finally came when the power was available. When the poles went up, the electrical cable was laid 1/4 of a mile to the generator, the aircraft warning lights were working and now the final installation of antennas could begin. Not two hours later, a Vietnamese garbage truck, making its daily run through the airfield, veered off the road, cut the electric cable just laid, and fell two of the 40 foot poles supporting the aircraft warning lights. Had the advisors not been pillars of virtue and possessed of great fortitude, this would have discouraged them. But, being ruthless, intrepid types, they had the cable spliced and the poles back in place in a matter of hours.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Finally, on St. Valentine's Day 1973, the metamorphosis of "mini-lake" was a reality and Can Tho's AN/TRD-23 MRDF site became operational. ARVN personnel, however, were not familiar with even the most basic maintenance procedures to support the site. Any outages that occurred were normally extended until TDY personnel from Saigon could diagnose the malfunction and acquire the necessary parts.

Inadequate maintenance capabilities not only plagued the MRDF site, but all facets of operations--vehicles, generators, air conditioners, commo/signal-equipment, etc. Since CTC was only permitted to perform first echelon maintenance, repairmen assigned received only limited training as opposed to the extensive schooling afforded their U.S. predecessors. As a result of limitations, any equipment malfunctions usually had an extended adverse effect on the entire operation.

As at any other field station, Can Tho's nucleus was the communications center (C.C.). Without this equipment running smoothly, the station was cut-off from the rest of the intelligence community.

Prior to January '73, W33's (intercept designator for CTC) C.C. experienced many maintenance problems. Because of cramped working conditions, maintenance personnel could not perform daily preventive maintenance (PM), which resulted in many operational hours lost. Recognizing the "cracker box" problem, advisors suggested to higher headquarters (Unit 15 - Saigon Center), that the C.C. at Can Tho be relocated to the area vacated by the U.S.C.C. This move would facilitate the following: first, daily PM could be performed, thereby eliminating approximately 50% of equipment down-time; second, the addition of three new circuits (two with Saigon/one with the proposed 44th Support Platoon) could be accommodated; third, a significant amount of circuitry and equipment was left by the U.S. communications people which would simplify the transition; fourth, the proposed area provided ample space to house all C.C. equipment and would also allow for further expansion should the need arise; and finally, the new area had the much needed direct air conditioning ducts to aid in keeping the equipment cool and operating. With Saigon's concurrence, the move was made and the C.C. began to run smoothly.

For any operations to run smoothly, constant supervision and guidance are necessary; therefore, every month the senior advisor accompanied the CO/CTC on his inspection tour to the

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

three subordinate ASTD's. These trips provided an on the spot review of equipment, personnel, problems at hand, and any foreseeable problems could be discussed.

Transportation was always the fastest, best mechanically tuned jeep available at CTC, while the ARVN driver was a conglomerate of Andy Granatelli, Richard Petty, Bobby Unser and Steve McQueen. This combination of driver and jeep was needed most on trips to the 7th ASTD located in Dinh Tyong Province. To reach the 7th from My Tho City, a spine-tingling drive along "ambush alley" (a stretch of road approximately 1000 meters long, flanked by thick jungle on both sides) was necessary. This was where jeep, driver and all occupants hoped for a new speed record on each and every trip.

These monthly sojourns into the VC/NVA occupied suburbs of the Mekong Delta, also allowed for sampling of the local culinary/gastronomical delights offered at the many roadside stands. These stands are known by many pseudonyms: "Ba muoi ba" stands (named after the Vietnamese Bier "33"), "Hepatitis Stands" (named after "post dinner complications"), and more commonly known to all as "the local Howard Johnsons". Inevitably upon their return to Can Tho, the ruthless, intrepid advisors proceeded posthaste (usually with a gait reminiscent to that of the "Green Apple Quick Step"), to the dispensary for a small white envelope humorously marked "Stop Gap", or "Cement Pills, for internal use only".

The successful transition from U.S. to ARVN COMINT operations has been evaluated and found satisfactory. The only unanimous regret, reflected by both ARVN and U.S. personnel involved, is that the VIM Program didn't begin earlier. Naturally, there is always room for improvement; but, keeping in mind the "newness" of the Vietnamese in the COMINT business, much credit must be given for their many accomplishments in such a short period of time. The advisors at Can Tho Center feel that the desire of the Vietnamese to constantly better the quality of their COMINT product will continue and enhance the overall Vietnamese Intelligence effort.

NOTE: The preceding article only high-lighted some of the achievements and humor associated with the Vietnamization Improvement and Modernization Program in IV Corps. To discuss the numerous anomalies and corrective actions that occurred on a daily basis would be cumbersome and would detract from the continuity of events. In reality, these daily occurrences often had the characteristics of the aimless wanderings of an odyssey and the futility of attacking windmills.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~CHRISTMAS AT THE SCHOOL

by Morris L. Ferguson, B43

On the first day of Christmas my Instructor gave to me:  
A Wired Rotor in a maze of three.

On the second day of Christmas my Instructor gave to me:  
Two Endplates steckering, and a Wired Rotor in a maze  
of three.

On the third day of Christmas my Instructor gave to me:  
Three Lobsters rolling, two Endplates steckering,  
and a Wired Rotor in a maze of three.

On the fourth day of Christmas my Instructor gave to me:  
Four Stem-Top Mushrooms, three Lobsters rolling, two  
Endplates steckering, and a Wired Rotor in a maze of  
three.

On the fifth day of Christmas my Instructor gave to me:  
Five Stepping Wheels, four Stem-Top Mushrooms, three  
Lobsters rolling, two Endplates steckering, and a  
Wired Rotor in a maze of three.

On the sixth day of Christmas my Instructor gave to me:  
Six Shrimp a-shrimping, five Stepping Wheels, four  
Stem-Top Mushrooms, three Lobsters rolling, two  
Endplates steckering, and a Wired Rotor in a maze  
of three.

On the seventh day of Christmas my Instructor gave to me:  
Seven Parallel Wires, six Shrimp a-shrimping, five  
Stepping Wheels, four Stem-Top Mushrooms, three  
Lobsters rolling, two Endplates steckering, and a  
Wired Rotor in a maze of three.

On the eighth day of Christmas my Instructor gave to me:  
Eight F's a=stripping, seven Parallel Wires, six  
Shrimp a-shrimping, five Stepping Wheels, four  
Stem-Top Mushrooms, three Lobsters rolling, two  
Endplates steckering, and a Wired Rotor in a maze  
of three.

\*

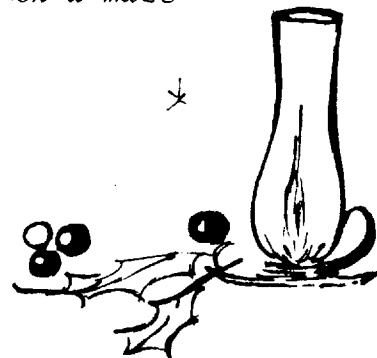
\*

\*

\*

\*

\*





~~TOP SECRET UMBRA~~

\*

\*

On the ninth day of Christmas my Instructor gave to me:  
 Nine Inverse Rod Squares, eight F's a-stripping,  
 seven Parallel Wires, six Shrimp a-shrimping,  
 five Stepping Wheels, four Stem-Top Mushrooms,  
 three Lobsters rolling, two Endplates steckering,  
 and a Wired Rotor in a maze of three.

On the tenth day of Christmas my Instructor gave to me:  
 Ten Diagonals running, nine Inverse Rod Squares,  
 eight F's a-stripping, seven Parallel Wires, six  
 Shrimp a-shrimping, five Stepping Wheels. Four  
 Stem-Top Mushrooms, three Lobsters rolling, two  
 endplates steckering, and a Wired Rotor in a maze  
 of three.



On the eleventh day of Christmas my Instructor gave to me:  
 Eleven Reflectors reciprocating, ten Diagonals  
 running, nine Inverse Rod Squares, eight F's  
 a-stripping, seven Parallel Wires, Six Shrimp  
 a-shrimping, five Stepping Wheels. Four Stem-Top  
 Mushrooms, three Lobsters rolling, two endplates  
 steckering, and a Wired Rotor in a maze of three.

On the twelfth day of Christmas my Instructor gave to me:  
 Twelve K's a-boxing, eleven Reflectors reciprocating,  
 ten Diagonals running, nine Inverse Rod Squares,  
 eight F's a-stripping, seven Parallel Wires, six  
 Shrimp a-shrimping, five Stepping Wheels. Four  
 Stem-Top Mushrooms, three Lobsters rolling, two  
 Endplates steckering, and a Wired Rotor in a maze  
 of three.



\*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

TIME TO LOOK AT PEOPLE

By Tom Glenn, B61

Many, perhaps most, of the organizations within B Group have been facing tough times lately. Billet cuts, some of Herculean proportions, and the resulting excess lists; moves from job to job; lack of promotions; and rife rumors of RIFS or worse--all have worked against us. The Director has asked us ("People Concerns," 12 October 1973) to give "compassionate, intelligent attention to the concerns of our people as a most important requirement of our management." It's high time we did.

According to the latest estimates I have been able to find (and these are hearsay--I cannot confirm them), NSA now spends more than two-thirds of its budget on salary; given the radically changing budget-salary ratio in years to come, we will soon reach three quarters. It would make eminently good sense, therefore, if we spent a commensurate amount of management time concerning ourselves with doing the right things to make our people effective and efficient. From my observations, I am convinced we do not, and the effects will come home to roost sooner rather than later.

Our stress in personnel management has consistently been on the external rules of operation vice common sense about what makes people work effectively. We spend enormous energy, for example, considering whether people fit the billet structure instead of whether the billet structure fits the people. We concern ourselves with numbers of people assigned in various categories instead of addressing who it is we need to get the job done. We have, in effect, created a myth world of personnel rules prodigious in their complete divorce from operational needs, and more important, from common sense approach to the concerns of people.

The impact on people of these rules has been less in the past than it is now, partly because we have never before applied them relentlessly and partly because the abundance of our budget in the past gave us slack and flexibility we no longer have. We have now learned, if nothing else, the disastrous effects on morale and productivity that unquestioning execution of personnel rules can cause. The problem is that we continue to do it anyway.

I am at a loss to understand why we do this. It may be partly because conventional wisdom dichotomizes concerns for productivity and concern for people (e.g., Blake-Mouton's management grid). But it takes little experience to stumble on the blunt truth

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

that in people organizations, people are the source of productivity. Only a feeble effort of the mind is required to carry the logic further--that people involved in problem solving or other creative endeavors (such as net reconstruction, code recovery, cryptanalysis, translation, report writing) do much better when they are happy than when they are not. In short, concern for productivity means concern for people so long as any initiative whatever is required.

But maybe we are really not concerned with productivity at all. As deranged as that sounds, I suspect that many an organization in B Group has not consciously addressed what it considers to be its output (its product, if you like) and how to measure it.

The inescapable conclusion of all this is that we in B Group must direct our foremost efforts towards our people vice things (collection gadgets, machine programs, telephone fixtures and typewriters). Unless, of course, we are really not concerned with productivity.

As must be obvious to the reader, I am abashed and puzzled by what I think I see going on. I'd be pleased to know the readers' thoughts.

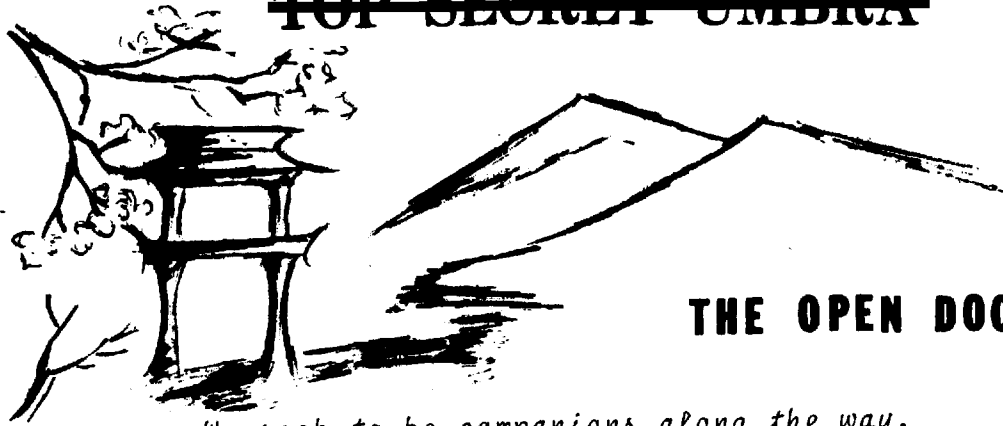
\* \* \*

*"If those who are excellent  
find no preferment,  
The people will cease  
to contend for promotion."*

---Lao Tzu

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



## THE OPEN DOOR

*We seek to be companions along the way.  
The lantern which we carry is not ours.  
The spirit which we share is contagious thought;  
The knowledge which we gain, an illuminating torch  
And all who seek may perceive and learn.*

*-The Concept of Dragon Seeds*

### ARE YOU USING COMPUTERS?

by Dr. Walter Jacobs

Does fear of the computer discourage you from using it to help you in your work? If so, you may be hurting your chances for advancement. You can accomplish much more when you properly use the computer than you can without it.

A person who distrusts computers may be subconsciously afraid the computer might take away his job. True, computers today are doing many things that, ten or twenty years ago, had to be done by people. However, these things are tasks that demand no judgment, and call for repetitive operations following consistent rules. Unless a job is challenging - unless it continually draws on the imagination, initiative and intelligence of the one doing it - it may be performed carelessly, inefficiently, and with limited attention. In that case it may be true that a computer can do it better.

In most jobs, however, a substantial amount of time is spent on routine and repetitious work. If much of this work can be turned over to the computer, more time and attention can be given to those aspects of the job that require experience and expertise. The work becomes more stimulating, and the product improves in quality and quantity.

When you begin to organize your work to make use of the computer, the fresh look you take at what you are doing can bring unexpected benefits. New and better approaches you may have overlooked could surface. A case in point happened in the field

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

of medical diagnosis and its implications for Agency professionals should be clear.

A project was set up in New York City, some years ago, to develop a computer procedure to do differential diagnosis of coronary heart disease; two expert heart specialists were selected to work on the project. There are 22 varieties of ailments involving the coronary arteries and their symptoms are often so similar that even specialists cannot be sure which is present; only surgery or - worse yet! - an autopsy reveals the specific trouble. In a set of actual cases assembled as data to be used in the project, the specialists were able to make an exact diagnosis in only 72 percent of the cases.

These specialists, working with an experienced systems analyst, developed a computer program that could reach a diagnosis from the type of information provided. Using the same data, the first program gave correct results in about half the cases. Applying continued effort over a period of two years, the specialists improved the procedure to the point where its score, on a new set of test cases, rose to about 70 percent. But the specialists themselves, with the sharpened understanding they had gained in the project, were nearly 90 percent correct on these new cases.

Of course, the computer procedure could not be relied on to replace a physician in doing diagnosis. It does seem clear, however, that the doctor could improve his diagnoses with the help of the program. Especially when it incorporates the experience and technique of the best practitioners, its contribution should enhance his own decisions, except where he simply accepts the computer results in an uncritical way. Perhaps a doctor who would do that ought to be replaced by the computer!

Learn about the computer programs that are available in your field. They may help you do a better job. Use them with understanding and judgment. Make improvements to the procedures where your knowledge allows you to do so. Your own career, as well as the Agency's work, will benefit.

\* \* \* \*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~MINNIE'S MINI

by Minnie M. Kenny



*It seems like ages ago when it all began. We were still at FANX and had just experienced the nine hundred and ninety-ninth power outage. No COPE, no RYE, no 6700, no NOTHING!!! To top it all off, it wasn't even raining. Now what kind of Providence is that?*

*We came up with an idea: why not hang a tape drive on that modified PDP-8 called the COPE terminal, boosting its memory by 4K, and declare our independence from Central Control? No way!! We got bottled up in channels and buried under paperwork.*

*That's when I began dreaming of desk-top terminals for C/A applications. Can't you imagine a user-controlled system of minicomputers, say one master and three slaves with an interchangeable hierarchy (to eliminate service interruption when there's a malfunction), and a terminal on each analyst's desk? Why you'd hardly need cross-section paper and pencils!*

*One day I stumbled across several idle CRTs. I was nosing around down in C at the time. I HAD to have them. Hooked up to one of the general processors, they'd make an adequate substitute for my dream system. I lost out again. I could pirate the terminals but I couldn't "bootleg" the hook-ups.*

*About this time, R came on the scene touting minicomputers with blisters. They were developing interactive C/A applications. And they wooed me with the promise of the realization of my dream. We formed a committee which formed a study group which formed into teams which inspected C/A processes in B. The results are discussed in the following article, but . . . I STILL WANT A MINI.*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

B NEEDS ITS OWN COMPUTER

by William P. Stivers, H11

Recently R conducted a 5 month study called ALBRECHT to determine whether an interactive computer need existed in B Group for the analysis of low/middle grade cryptosystems. A five member study group composed of one member each from R111, R113, R252, R313 and a CA intern with experience in B1 determined that such a need did exist. The study group found that with an interactive computer many of the B target systems could be solved more efficiently and the time and versatility gained could be aimed at solving other B target systems. The formal ALBRECHT STUDY report explains how the study was conducted and describes a computer system that would provide the interactive capability needed in B. This article is a review of the main sections of the ALBRECHT report and is especially intended for those who may not read the formal report.

The ALBRECHT study began with visits to analysts in B1 to see the types of CA problems being worked and the techniques used in attacking the problem. ALBRECHT visits focused on B1 because earlier tasking, prior to the reorganization and physical moves, had emphasized looking at that organization. The types of CA problems being worked included diagnosis of unknown systems, recovery of parameters of diagnosed systems, and decryption.

In the first type of problem, diagnosis, an interactive system would facilitate the processes by instantaneously providing STET statistics while at the same time offering versatility to rapidly manipulate the data for other tests. For instance, if the tests indicated significant scores for a particular width, the analyst could quickly and simply display the message on that width. If null groups were suspected they could be edited out of the message with a few simple statements. Each analyst could develop, for his own data, countless displays and tests, all of which would be rapid in execution and yet relatively simple in construction.

The second class of problems, parameter recovery, is especially suitable for attack by an interactive computer. Here, where the "modus operandi" is trial and error testing of assumed parameters, the interactive system would provide a rapid means for testing these assumptions. For instance, an analyst working a problem diagnosed as transposition; but with an unknown width and key, could repeatedly display the text on a

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

scope according to assumed widths and keys. After each display the analyst would base his next assumption on observed digraphic properties and other latent patterns, until plaintext started forming. In a chart system where a particular cipher group had several possible meanings, the analyst could rapidly test each assumed meaning to determine which one was most likely correct. Numerous other situations involving trial and error procedures with human intervention for decision making are done most efficiently on an interactive system.

The third class of problems, decryption, is not a prime candidate for attack by an interactive computer. If all the parameters are known and the decryption process can be put into a clearly defined algorithm, the problem is better solved on a compiler system without interaction. If some of the parameters are sketchy, however, or if they are subject to frequent change, the interactive system could again be a useful tool.

During the visits to BI, ALBRECHT also observed some non-cryptanalytic problems that confront the analysts on a daily basis. For instance the analysts have a problem of storing message hard copies, data paper tapes, data and program cards, cipher and code charts, and other miscellaneous program runs. Most of the storage is in desks, cabinets, and boxes where retrieval after any period of time longer than a week becomes cumbersome. With an interactive computer having large file capability, the analyst could store much of the above materials in files, and quick retrieval would be an elementary procedure. Editing was also cumbersome when data had already been punched on paper tapes or cards. Often, if the analyst wanted to add or delete characters or non-textual groups the data had to be repunched. In an interactive computer system, editing chores such as changing, adding, or deleting characters and groups are simple matter-of-fact operations. Another problem the analysts faced was the incompatibility of the machine aids being used. There was a RYE terminal with paper tape input, a 360 COPE terminal with card input, and a Burroughs outstation which also had card input but with special character punches different from those of the COPE terminal. A file-structured interactive system where programs and message texts could be stored in files would eliminate the incompatibility problem. The analyst could do all the work at one terminal using files which had been created from desired peripheral input devices.

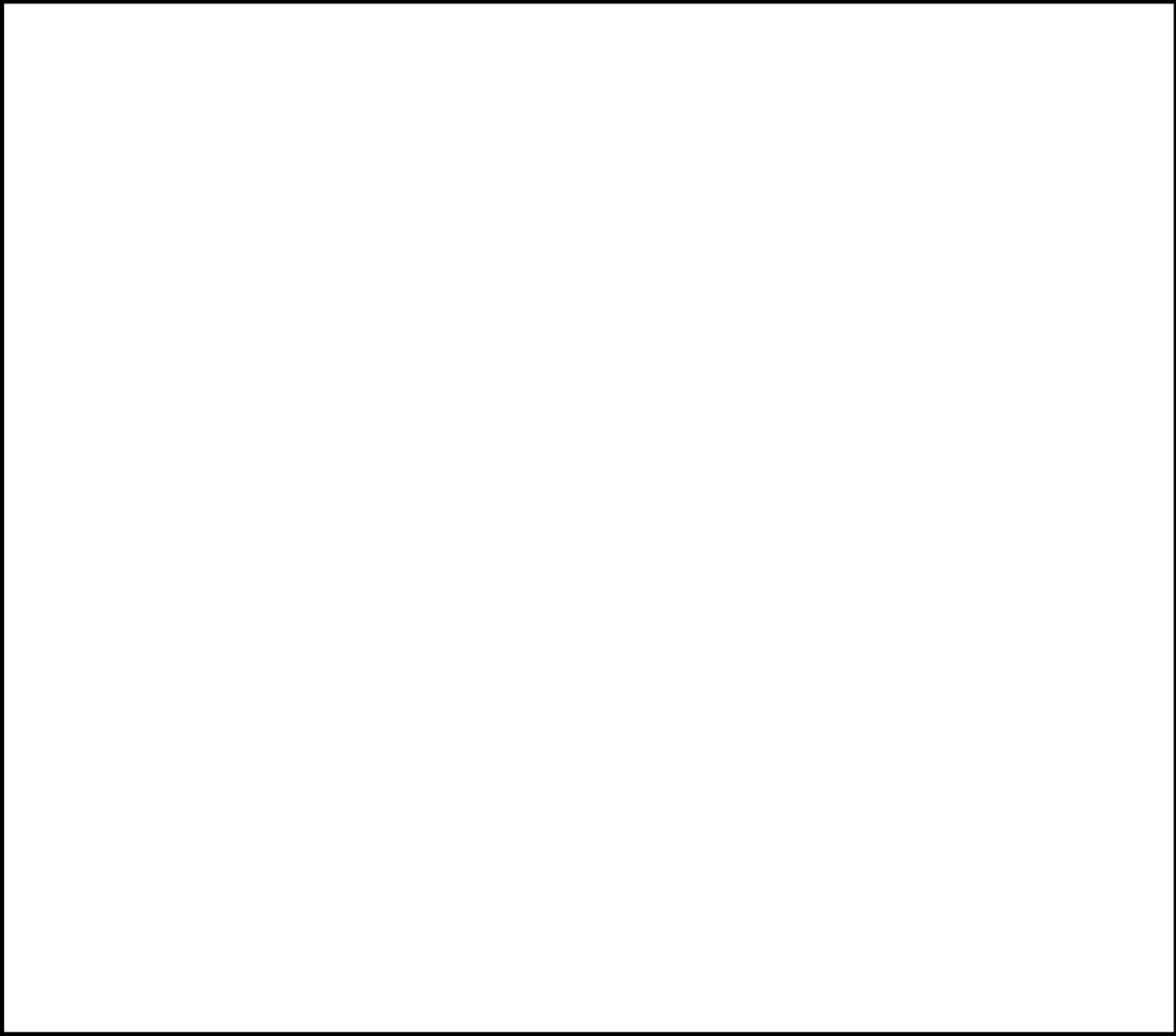
~~TOP SECRET UMBRA~~



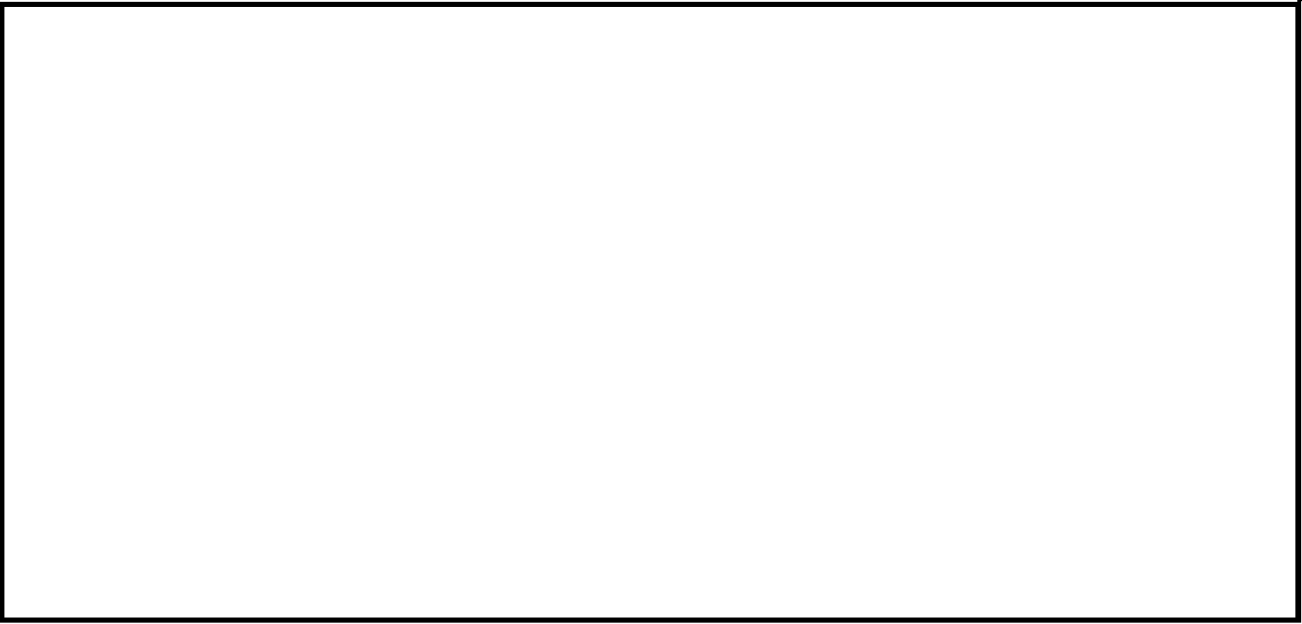
~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

After visiting the analysts in B1, members of ALBRECHT wrote APL programs for some of the CA problems they had observed. The particular problems chosen were not the only ones suitable for interactive attack, nor were they considered the best candidates for interaction. They were simply chosen out of interest. The study group used APL to program the problem because it is a truly interactive language and facilities for its use were convenient.



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

In each of the demonstration problems programmed by ALBRECHT, the advantages gained in continual accuracy and time saved were sizeable. The human intervention for decision making, which usually took the place of a branch that could not have been canned in a neatly defined algorithm, was the predominant asset of the APL program.

Along with the visits to B and the demonstration programs, the ALBRECHT study continued with technical demonstrations, briefings and directed research. Then, prior to stating the actual system recommendations, the study group made some general observations, the main area of which dealt with programming languages. Three languages, APL, FORTRAN, and BETA, were mentioned though ALBRECHT did not experiment with FORTRAN and BETA; FORTRAN because it was not felt necessary and BETA because it would have delayed the study to learn it, resources were not readily available, and in no way was it the intention of the study to evaluate BETA.

APL is a truly interactive language that permits human intervention for decision making and redirection of the program. Its mathematically oriented symbolism allows experienced programmers to write concise statements to perform the desired analysis. The ease of character handling and the ease of array-structured data manipulation make APL attractive to the CA analyst programmer. APL is ideally suited for short lived problems where the advantage of decreased programming time outweighs the consideration of CPU

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

time. This is important in B Group where ALBRECHT has observed that some of the demonstration problems programmed by the study group have already died. APL is also well suited as a test vehicle for new ideas or problems.

FORTTRAN is a well known and widely used compiler language. Versions of FORTTRAN, more or less compatible with each other, exist on all computer systems. Being a compiler it produces efficient code and is well adapted for longer running jobs. FORTTRAN certainly should be on any NSA system.

BETA is an NSA developed and maintained compiler language. It is oriented toward character and bit stream manipulation and cryptologic processes. Since ALBRECHT never experimented with BETA it cannot comment on BETA's overall desirability or how easy it is to use or learn.

At the conclusion of the 5 months of study ALBRECHT made recommendations for a system to meet B's interactive needs. ALBRECHT suggested that B Group be given definite access to a medium-to-large general purpose computer. The system should be file-oriented time sharing with a large file storage capability. The file storage capability must be large (perhaps as much as 32 million bits/user) since most of the data handling problem would be eliminated if all current and many past messages and analyst's programs could be stored in files.

The ability to create, edit and peruse the files from the terminal is deemed a necessity for the proposed system. The files must be easily spliced together and they must be easily linked as input to any job executed in any mode or written in any system language. The linked files may be submitted at the terminal as either a time-sharing job (immediate run) or as a batch or background job.

The essential programming languages for the system are FORTTRAN, APL and assembly language.

Batch mode processing should be initiated at the terminal using files. Also, the analyst should be allowed to decide by inspecting an output file whether the output should be sent to the line printer.

The analyst should have ready access to the terminals and most of the terminals should be of the CRT (cathode ray tube) type with identical keyboard and character sets. With a file oriented system using CRT's, much of the hard copy output can

~~TOP SECRET UMBRA~~

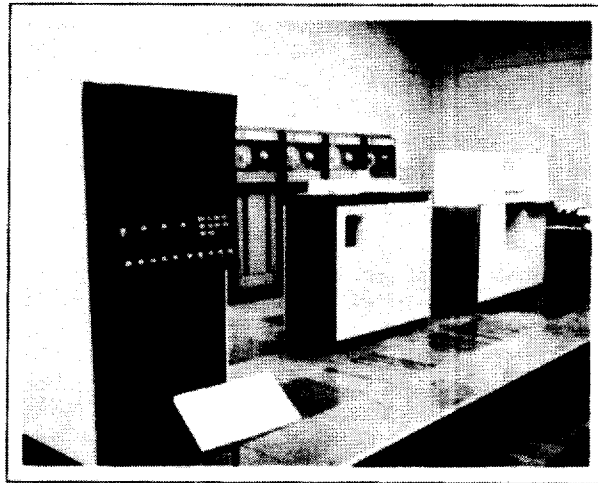
~~TOP SECRET UMBRA~~

be suppressed, but it is still essential to have hard copy output readily available. A system line printer is essential and one or more typewriter terminals and/or device(s) that reproduce the CRT screen by photo-copy could be provided.

All character data throughout the system, whether in core, in file storage, or in passing from or to the peripherals or terminals should be in compatible form.

ALBRECHT also suggests that B Group secure several 370 APL terminals as an intermediate action while pursuing the above proposed system. The 370 APL terminal is a powerful analytical tool and its introduction into B Group would significantly enhance B's cryptanalytic effort.

\* \* \* \*



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



~~S SPOKE~~

FM DIRNSA

TO USM-7

~~S E C R E T SPOKE~~

+B65-1248-73

CAMBODIAN PROCESSING

YOUR 260730Z NOV 73

1. THE FRENCH ABBREVIATION GRUNC EXPANDS QTE GOUVERNEMENT ROYAL D'UNITE NATIONALE DU CAMBODGE UNQTE QTE GRUNK UNQTE EXPANDS GOVERNEMENT ROYAL D'UNITE NATIONALE DU KAMPUCHEA UNQTE. BOTH XLATE QTE ROYAL GOVERNMENT OF THE NATIONAL UNION OF CAMBODIA UNQTE. QTE RGNUC UNQTE IS THE ENGLISH EQUIVALENT OF GRUNC/GRUNK. WHEN ABBREVIATION QTE GRUNC UNQTE OR QTE GRUNK UNQTE IS OBSERVED IN A MSG. PLS USE APPROPRIATE ABBREVIATION IN XLATION AND FOOTNOTE QTE ROYAL GOVERNMENT OF THE NATIONAL UNION OF CAMBODIA UNQTE. GRUNC OR GRUNK ARE THE ACCEPTED ABBREVIATIONS FOR CAMBODIAN PRODUCT.

XGDS 2

\*\*\*\*\*

REVIEWED BY N. P. MOORE, D/CH, B651/MR. LEE, B65

CONCUR B609, MR. JAMIESON

B09, MR. CHASE

B, B6, B65, B7, G923, ASALNGP

W. R. NIEDERHAUSER, B6512, 7196S GEOFFREY C. WOOD B65 7178S

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

[REDACTED]

by Russ Myers, B65

Some years ago it was discovered that the majority of code reconstruction problems could be serviced by a general-purpose package of programs. This discovery led to the development of the Bookbreaker's Package which, in its Version 1, fulfills the analyst's minimum initial machine run requirements. The package, designed in C53 (now G46) in close cooperation with bookbreakers from G, parallels Swift's *Standard and Techniques of Code Reconstruction*. Its Version 1 provides a standard bookbreaker's index, a beginnings sort, an endings sort, a decoded vertical message print, a message header log, and listings of all recovered code groups residing in the code meaning file in inverse frequency order, decode order, line-page order, and encode order. There also exists a Version 2 which permits the updating of message and meaning files and a Version 3 which provides for a Decoded Bookbreaker's Index (the meaning for a code group, when available in the meaning file, is substituted for all occurrences of that code group in indexed text).

A more recent programming effort by Mr. Bill Davis of B209 for bookbreakers of Chinese-language codes, produced the Text Index procedure.

[REDACTED]

At the direction of Ms. Minnie Kenny, B4 TDLA, a procedure has now been developed to combine the best features of both the Text Index procedure and Version 1 of the Bookbreaker's Package. Mr. Mike Fresty, formerly a Data Systems Intern in B65 and now permanently assigned to G46, was selected by Ms. Kenny to provide the IBM370 JCL and POGOL language changes necessary to link the two procedures. Although the procedure was originally prepared to assist B21 bookbreakers, it can be used with little modification, for any tetronomic code whose messages are resident in an AG-22/STRUM data base.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Essentially, the new procedure has all features of Text Index up to the creation of horizontal message prints. These are stored on an intermediate disk file in a format compatible to that required by the Bookbreaker's Package. A call is then made to the Bookbreaker's Package to produce all Version 1 outputs.

The procedure has been setup to run via COPE RJE; however, it should be noted that when a significant volume of data is involved, the procedure should be run at the IBM370 mainframe. In its present form, the procedure will not allow the user to selectively produce output options of the Version 1 Bookbreaker's Package; however, relatively minor changes i.e., insertion of dummy cards, could accommodate such a requirement. Additionally, the SPECOL language selection criteria composed by the user must be such that he can assure a run against a homogeneous set of data. The most readily available retrieval fields are date, case notation, and cryptosystem title. For full effectiveness, when discriminating among cryptosystems, the user should assure that either a "front-end" weighting routine is used or that the specific cryptosystem title is inserted in the appropriate field through data base file maintenance.

For additional information on this new procedure, contact Ms. Kenny of the B4 Technical Directorate, room 7A144 (5414s).

\* \* \* \*

TD QUOTES -

*"It seems that 2/3 of the people we hire in this Agency are to throw roadblocks in the way of progress."*

--- G. S.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

----SEEK THE BIZARRE SOLUTION -

Are you thinking about better ways to do your job?  
 Are you frustrated because your good idea would require too many others to change their ways?  
 Are you tired of doing it by hand when the machine could and should do it faster?  
 The Technical Directors want your ideas on how B can work together to do the job better. No suggestion for improvement is too outlandish or bizarre to consider. Call us:

LANGUAGE	- 5414s
CRYPTANALYSIS	- 5978s
TRAFFIC ANALYSIS	- 5978s
AUTOMATED SYSTEMS	- 5007s

\*\*\*\*

----ANNOUNCEMENTS OF CMI AND CLA ESSAY CONTESTS. CMI ESSAY CONTEST - RULES SLIGHTLY REVISED. Papers are now being accepted for the 15th annual CMI Essay Contest. All entries should be submitted to Miss Judy Bennett, G4, 3A114, extension 3109, no later than March 29. Type-written manuscripts are preferred, and three copies should

be submitted. Necessary diagrams or drawings should be included.

The purpose of the contest is to recognize professional accomplishment and to foster documentation of new and/or important ideas in cryptomathematics. At the annual CMI banquet, prizes of \$100, \$50 and \$25 will be awarded in accordance with the recommendations of the panel of judges. All entries submitted will be considered for publication in the NSA *Technical Journal*.

All NSA employees, including non-members of the CMI, are eligible to enter the contest. In addition, any member of the CMI who is not an NSA employee may also enter. Papers may be submitted on behalf of their authors, providing the author is eligible and consents.

Any writing on cryptology or a significantly related topic may be entered. Security classifications are permissible. Compartmented papers will not be accepted, but any techniques or ideas originating in compartmented

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

problems may be reduced to a noncompartmented level. All NSA *Technical Journal* articles of the current contest year will be automatically considered as entries.

Papers published outside NSA are also acceptable as entries. Authors may wish to perform some revision or addition to make the relevance of the subject to cryptology or related topic more explicit. If such relevance to cryptology is not or cannot be supplied, judges may use its absence as a primary reason for eliminating the paper from further consideration.

The CMI will select the panel of judges whose names will be announced when all papers have been submitted. Judges of the contest are not eligible to enter. Criteria for judging are: a) Relevance to mathematics and cryptology, b) Significance of the content to Agency operations, c) Interest of the paper to Agency professionals, d) Quality of the writing.

#### CLA ESSAY CONTEST

The eighth annual essay contest of the NSA Cryptolinguistic Association is now open, and papers will be accepted until March 15th, 1974. The purpose of the contest is to encourage writing on topics concerning the application of linguistic knowledge to the solution of Agency-related problems so that organized information can be

disseminated among professionals in this field. At the spring meeting of the CLA prizes of \$100, \$50 and \$25 will be awarded in accordance with the recommendations of the panel of judges. All entries submitted will be considered for publication in the NSA *Technical Journal*.

Any NSA employee, regardless of his membership in the CLA, is eligible to enter the contest. In addition, any member of the CLA who is not an NSA employee may enter. Papers may be submitted by others on behalf of their authors, provided the author is eligible and consents. Judges, however, are not eligible.

Any writing on cryptology or a significantly related topic may be entered. Security classifications up to and including TSC are permissible, but techniques and ideas originating in compartmented problems must be reduced to a noncompartmented level. All NSA *Technical Journal* articles of the current contest year will be automatically considered as entries unless they have been considered in a previous contest.

Typewritten manuscripts are preferred, and three copies should be submitted. Necessary diagrams or drawings in finished form should be included.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Papers should be submitted to Mrs. Constance H. Grisard, G94, Room 2S010, Operations Building #1, extension 4812s.

The CLA will select a panel of judges whose names will be announced when all the papers are in. Criteria for judging are:

- a. Relevance to cryptology of the subject and treatment,
- b. Interest of the paper to Agency professionals, and
- c. Style of writing.

Papers published elsewhere (outside NSA or in the NSA *Technical Journal*) are acceptable as entries. Authors may wish to perform some revision or addition to make the relevance of the subject to cryptology or related topic quite explicit; it may not have been necessary or possible to do so in the original publication. References to the areas where the problem occurs or where the ideas can be applied may well be incorporated into contest submissions so that judges and other readers do not have to supply this pertinent information. If such relevance to cryptology is not or cannot be supplied, judges may use its absence as a primary reason for eliminating the paper from further consideration.

Compartmented papers will not be accepted, and any work which because of its length would not be suitable for publication in the NSA *Technical Journal* will not be accepted.

\*\*\*\*

----Have you tried CANDE??  
It's out of sight!!  
You should see what Russ Myers and cohorts in B65 are doing in the way of interactive C/A applications. Why don't you call him and get a demonstration? That's 3447s.

\*\*\*\*

----LANGUAGE TESTING SYMPOSIUM  
13, 14 March 1974

(Immediately preceding the  
Georgetown Roundtable)  
New South Faculty Lounge  
Georgetown University  
Washington, D. C.

Sponsored by member of the United States Government Interagency Language Roundtable (Foreign Service Institute of the Department of Defense, Office of Education of the Department of Health, Education and Welfare, Central Intelligence Agency, National Security Agency), the Center for Applied Linguistics and the Commission on Tests and Testing of the International Association of Applied Linguistics (AILA).

Purpose: To explore problem areas of testing language proficiency as it relates to the use of foreign languages on the job. Among the topics of discussion will be: the oral interview test, remote testing of speaking proficiency, cloze testing, reduced redundancy testing, criterion-referenced testing and subjective vs. objective language

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

tests. During each of the four sessions of the symposium two or three presentations will be made. Each presentation will be discussed in detail by a panel of invited participants.

The public is cordially invited. If you would be interested in attending, please fill out the registration form and return it by 22 February 1974. There is no charge for registration. A complete program will be sent by 1 March.

All arrangements for lodging and meals will be the responsibility of each individual. Information about hotels and motels in the Georgetown area will be sent on request. Registration form should include Name, Address, Country, and Institution. Please indicate if you need hotel information or further information about the Georgetown Roundtable. Return completed forms to:  
LANGUAGE TESTING SYMPOSIUM  
P.O. Box 9569  
Rosslyn Station  
Arlington, Va. 22209

\*\*\*\*

----Did you know that copies of Communist Propaganda Highlights prepared by the Psychological Warfare Research & Intelligence Division are now available in the B Language Media Center, Room 3S078? See George Sing, ext. 5309s/5310s.

\*\*\*\*

----Future CMI Lectures:

7 March 1974 - Mr. E. Speigelthal, R111, "Representation of Integers - A Linguistic Problem."  
4 April 1974 - Prof. S. Kullback, George Washington University, "Contingency Table Analysis."  
2 May 1974 - Dr. N. Zierler, IDA, "A Computational Problem in Finite Fields."  
17 May 1974 - Prof. J. Tukey, Princeton; Bell Telephone Lab, Topic to be announced.  
6 June 1974 - Mr. T. Evans, Pl, Topic to be announced.

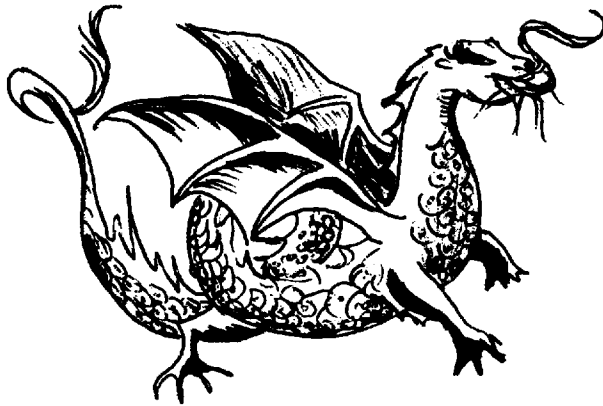
\*\*\*\*

----C announces a new programming system for the CDC 7600 and IBM 370 computers. The programming system is BETA. This is a tool expressly designed to aid analysts in solving their cryptologic problems.

Many Agency personnel are using earlier versions of BETA on IBM and BURROUGHS equipments. They find it to be extremely useful in their work. With BETA available on BURROUGHS, CDC, IBM, and soon UNIVAC computers, Agency analysts now have a variety of hardware choices to meet their programming requirements.

\*\*\*\*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

ASK  
THE  
DRAGON  
LADY

Dear Dragon Lady,

Mr. Glenn's letter of last month raises a valid point concerning insights into the organization and functions of the Central Reunification Committee gleaned from SIGINT during 1958-62. However, in contrast to Mr. Glenn's suspicion, recent plaintext Civil messages reveal that the CRC is still with us, alive and well somewhere in North Vietnam, and actively involved with South Vietnamese affairs. Ms. Kennard's basic observations concerning the role of the CRC provoked us to research its current posture. We found her equation of the CRC to CP. 40 questionable in light of recently consolidated material dating from the early 1950's to the present. We are still synthesizing a large volume of SIGINT hoping to determine the CRC's present relationship with the Lao Dong Party, COSVN, the SVNLA, NVN governmental and administrative control of liberated areas in SVN and the like.

Peter J. Melly, B614

\* \* \* \*

In the continuing discussion of the linguist's plight, the Dragon Lady offers the following in an effort to refute the oft repeated equation that a "warm body + dictionary = Linguist", and to explain the Language Analyst's constant quest for the latest, most up-to-date reference works. The thoughts were excerpted from *Word Play* (Alfred A. Knopf, publisher) by Peter Farb, an anthropological linguist, former lecturer in English at Yale University, and author of several books.

*". . . In short, every language offers its speaker an array of strategies with which they can play the language game. . .*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Most people assume that a text in one language can be accurately translated into another language, so long as the translator uses a good bilingual dictionary. But that is not so. . .

Despite what most people believe, dictionaries do not give the "meanings" of words. Rather, dictionaries present "meanings" by offering a selection of synonymous words and phrases - which are themselves listed in the dictionary. The dictionary thus is a closed system in which someone interested in the meaning of a word can go around and around and end up exactly where he started, simply because words are defined in terms of other words, and these, in turn, are defined in terms of still other words. . .

The "meaning" of a word in the dictionary, therefore, is not the meaning at all. It serves merely as a reminder to a speaker WHO ALREADY KNOWS HIS LANGUAGE<sup>1/</sup>, has grown up in a speech community that uses the word, and who employs the hints in the dictionary to make a guess at the meaning. . .

Finally, an adequate dictionary usually takes at least a decade to prepare (the OXFORD ENGLISH DICTIONARY required about 50 years), and by the time it has been completed it is the dictionary of a changed language, simply because the meanings of words do not stay the same from year to year."

1/ capitalization supplied

\* \* \* \* \*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

## SOLUTION TO SEPTEMBER'S PUZZLE:

0926 9704 1899 7956 9489 0926 2939 8303 1722 1125 1172 7567  
 4102 5363 7831 2397 9976 4102 1367 3630 0849 4104 2455 6859  
  
 9489 1604 4436 3281 7352 5089 7984 0184 0252 1562 1624 3281  
 9976 2508 0191 6651 5669 5890 4099 1455 0735 4430 1331 6651  
  
 4381 1126 1172 7567 9489 1604 4436 3281 2236 0342 1126 1387  
 2975 4104 2455 6859 9976 2508 0191 6651 2053 0948 4104 4357  
  
 3084 1409 2559 4813 0156 2326 0187 1126 1172 7567 9390 7352  
 2585 0031 5030 2429 0553 4907 2837 4104 2455 6859 9975 5669  
  
 5089 5472 0103 2851 1126 4224 0324 0252 9725 9372 1551 0019  
 5890 0006 0008 0681 4104 1748 1709 0735 7364 2706 0668 0110  
  
 8718 8906 7984 0184 9489 1562 1624 5472 0103 2851 1126 1624  
 5261 3945 4099 1455 9976 4430 1331 0006 0008 0681 4104 1331  
  
 4858 1551 0019 8718 8906 8303 3181 9390 2911 3351 8169 7771  
 3175 0668 0110 5261 3945 3630 6158 9975 0448 3938 5887 2398  
  
 7154 3874 9489 1326 0771 2057 8169 5455 2780 9725 9372 9489  
 0500 6852 9976 1730 0455 2236 5887 0001 4467 7364 2706 9976  
  
 5455 2780 1624 4858 9489 4687 1393 1539 5455 2780 9725 9372  
 0001 4467 1331 3175 9976 4391 2972 0659 0001 4467 7364 2706  
  
 9489 1539 5455 2780 1624 4858 9489 2236 0015 4143 5321 3084  
 9976 0659 0001 4467 1331 3175 9976 2053 0226 6126 3634 2585  
  
 6450 6317 1870 7352 5089 0252 2780 1624 1126 7984 0184 9390  
 2589 1364 2456 5669 5890 0735 4467 1331 4104 4099 1455 9975  
  
 7352 5089 0252 2780 1624 0120 1126 1604 5470 4656 9514 9489  
 5669 5890 0735 4467 1331 0022 4104 2508 7236 0795 7344 9976  
  
 2210 7651 3276 7761 7352 5089 2072 2780 1624 2072 1126 8718  
 2019 3981 6639 6665 5669 5890 3954 4467 1331 3954 4104 5261  
  
 8906 7742 3181 0157 6629 4274 9489 3276 7761 7352 5089 0252  
 3945 6062 6158 0637 6043 3082 9976 6639 6665 5669 5890 0735  
  
 2780 1624 1126 4670 1779 0157 6629 4274 9489 8940 0103 2210  
 4467 1331 4104 1395 6432 0637 6043 3082 9976 5079 0008 2019

(Continued next page)

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

7651 5011 2724 2988 0426 1126 1172 4814 0157 6629 4274 9390  
3981 2231 0648 4675 0830 4104 2455 3127 0637 6043 3082 9975

PLAYFAIR SQUARE

00 01 05 06 14 15 27 28 44 45  
02 04 07 13 16 26 29 43 46 63  
03 08 12 17 25 30 42 47 62 64  
09 11 18 24 31 41 48 61 65 78  
10 19 23 32 40 49 60 66 77 79  
20 22 33 39 50 59 67 76 80 89  
21 34 38 51 58 68 75 81 88 90  
35 37 52 57 69 74 82 87 91 96  
36 53 56 70 73 83 86 92 95 97  
54 55 71 72 84 85 93 94 98 99

\* \* \* \*

TD QUIPS -

*"Anytime you let the shape of the vessel determine the contents, you ARE in trouble."*

-- H. G.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

## CONTRIBUTORS

MORRIS L. (LEROY) FERGUSON, B43, came to NSA in December 1963 after a three-year tour in the Army. He worked in A5 until 1970 when he entered the Cryptanalysis Intern program. Leroy graduated from the Intern program in December 1973 as a certified cryptanalyst and was assigned to B43. He is currently attending Mr. Callimahos's CA400 class.

TOM GLENN, Chief, B61, has a total of 15 years' experience with ASA and NSA on the Vietnamese problem. He is a professional Special Research Analyst and Vietnamese linguist who has also studied Chinese and French on his own. Mr. Glenn has served as the Chairman of the Vietnamese Language Professionalization Examination Committee. Assigned to Vietnam in 1962-65, 1967-68, and 1969, he has been involved in traffic analysis, cryptlinguistics, intelligence analysis, and most significantly, in the management of the SIGINT reporting effort on the Vietnam war. In December 1973, Mr. Glenn received his M.A. in Government at George Washington University.

WALTER W. JACOBS retired as COMMANDANT, National Cryptologic School, in October 1969 to join the faculty of The American University. He served as Chairman, Department of Mathematics and Statistics, from June 1970 to June 1973 and is at present heading the Computer Science program at the University. Dr. Jacobs comments, "What a great place the Agency is -- an unusual group of people with outstanding ability, dedication, talents, and variety of interests -- there's nothing like it on the outside!" For the past two summers, Dr. Jacobs taught an advanced programming techniques course at NSA and hopes to teach for the Agency again this summer. After Dr. Jacobs earned his PhD in Mathematical Statistics at the George Washington University, he had Military Service during World War II in the Office of the Chief Signal Officer (OCSigO) at Arlington Hall and Bletchley Park (England). Later, he served in key civilian positions involving mathematics in the USAF, in the R&D Organization of NSA, and as Chief of the NSA Machine Organization, then C4, from 1961-1963.

RUSS MYERS, B65, joined the Agency in 1965 after serving four years with the USAFSS. Fifteen months of his Air Force tour were spent at Peshawar, Pakistan, one of the "garden spots of the world." At NSA, he spent two years in A8 as a traffic analyst and Russian linguist and then was selected for Class 10 of CV100. He moved to B1203 (now B6503) in 1968 as a

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

cryptanalyst. Mr. Myers was a member of Class 24 of CA-400 and was detailed for six months to B42 under the B Internal Data Systems Training Program. He holds professional certification in traffic analysis, cryptanalysis, and computer systems analysis, as well as a BA in Government and Politics from the University of Maryland. Mr. Myers is currently involved in the development and management of several data processing projects for B65 problem areas.

EDWARD A. O'CONNOR served with the Air Force Security Service after receiving a Bachelor of Arts degree from Rhode Island College in 1966. He joined NSA in May 1970 as a Traffic Analytic Technician and in 1971 he was selected for an internship by the Traffic Analysis Career Panel. Currently, Mr. O'Connor is a member of UNCOAST.

WILLIAM STIVERS has been with NSA seven years, the last two of which he has spent as a CA Intern. Prior to joining the Intern program, he was assigned to the [redacted] where he gained experience in signals analysis as well as cryptanalysis. He acquired an interest in programming as an analytical tool during Intern tours which required a programmer analyst. Bill believes in doing things the hard way and, accordingly, is attending Towson State Evening School where he is a Junior.

LEO C. STEPP, B632, joined NSA in 1965. He has been involved with the Vietnamese Communist problem almost all of his Agency life. From July 1972 to June 1973, Mr. Stepp served as the Senior U.S. COMINT Officer and Advisor to the South Vietnamese Special Security Technical Branch in MR IV (Can Tho, SVN). He is currently assigned to B632 as a member of a team responsible for [redacted]

JACK THOMAS, B44, came to NSA as a CIVOP in 1956, after a 3-year tour in the Army Security Agency. He holds a degree with a major in English. In addition to his initial Agency assignment as a CIVOP at Herzo Base, Germany, he has worked in predecessor W organizations, at the Pacific Experimental Facility in Japan, and since 1966 in B4. He is now on a History Fellowship with the National Cryptologic School Press, and has recently been appointed to the Editorial Board of the Cryptologic Spectrum.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

비밀  
한  
것  
이  
다



IT'S CLASSIFIED !!!!

~~TOP SECRET UMBRA~~

~~TOP SECRET~~

# National Security Agency

Fort George G. Meade, Maryland



MARCH 1974



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~TOP SECRET UMBRA~~

This is *Dragon Seeds*.

There is fantasy, irony, and the bite of reality in the name. It speaks of the East. And, like the East, it suggests much, says little.

*Dragon Seeds* is both Mother China and her neighbors. *Dragon Seeds* is monumental and minuscule. It is the past and future. It begs for elaboration but gives none. In it are echoed softly slurred Mandarin, brittle Vietnamese, determined Korean. In it is the spectre looming over the Thai, Lao, and Khmer. It is frightening and friendly. It is uncertain.

Above all, *Dragon Seeds* is promise. It is fertile with ideas unbounded, to be cultivated with creativity and imagination. It is challenge. It is alive. It will be more than it is.

*Dragon Seeds* is yours. May it grow with you.

The Editors

~~TOP SECRET UMBRA~~

DRAGON SEEDS

Publisher

DONALD E. MCCOWN, CHIEF B4

Managing Editor  
Minnie M. Kenny

Executive Editor  
Robert S. Benjamin

Rewrite Editor  
Jane E. Dunn

Special Interest Editor  
Ray F. Lynch

Feature Editor  
Robert F. Kreinheder

Education Editor  
Marian I. Reed

Composition

Louella M. Ertter

PRESS CORPS

B11 Carolyn Y. Brown

B42 Peggy Barnhill

B2 George S. Patterson

B43 Mary Ann Laslo

B31 Jack Spencer

B61

B32 Jean Gilligan

B62 Edmund J. Guest

B33 Louis Ambrosia

B63 William Eley

B41 James W. Schmidt

B65 Philip J. Gallagher



~~TOP SECRET UMBRA~~

WHAT OTHERS TAUGHT  
I ALSO TEACH.

THE KNOWLEDGE OF CONSTANCY  
I CALL ENLIGHTENMENT AND SAY  
THAT NOT TO KNOW IT  
IS BLINDNESS THAT WORKS EVIL.

至  
聖  
先  
師



BE DONE WITH ROTE LEARNING  
AND ITS ATTENDANT VEXATIONS!

BY THIS I KNOW THE BENEFIT  
OF SOMETHING DONE BY QUIET BEING;  
IN ALL THE WORLD BUT FEW CAN KNOW  
ACCOMPLISHMENT APART FROM WORK,  
INSTRUCTION WHEN NO WORDS ARE USED.

---Lao Tzu

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~
A NATURAL HISTORY OF GUPPIES

Virginia Jenkins, E13

The GUPPIES on RYE are a collection of over one hundred computer programs, designed and for the most part written by cryptanalyst programmers, to handle many of the standard cryptanalytic tasks performed daily throughout the Agency. The name "GUPPY" comes from the initials of General Utility Programs. This article tells in brief how general cryptanalytic programs, cryptanalyst programmers and remote-operated computers grew up together at NSA.

ROGUE, ROB ROY AND RYE

The GUPPIES were born (but were not yet named) with ROGUE,<sup>1</sup> NSA's first remote-operated computer system, in 1956.<sup>2</sup> Open-shop programming--programming of their own work by local analysts--started at about the same time. It seems to have been realized rather early that cryptanalysts who could program their own jobs had a valuable tool in their tool boxes, and that the best desk-side aid for any cryptanalyst was a computer program he could run himself from his working area. ROGUE provided both possibilities. It boasted four outstations.

The tradition grew, and so did the number of users, open-shoppers, and programs. The five outstations of ROB ROY,<sup>3</sup> which succeeded ROGUE in 1960, were busy and productive. ROB ROY was popular in spite of long waits for input, one-job-at-a-time processing, and paper tape as the only mode of output.

1. Remotely-Operated General Use Equipment. The computer was the ALWAC IIIIE.

2. ROGUE in fact was one of the first in the country. Monograph #2 in the NSA Technical Literature Series, HISTORY OF NSA GENERAL-PURPOSE ELECTRONIC DIGITAL COMPUTERS, by Samuel S. Snyder, tells the story. Some of the information in this article is based on that monograph.

3. The computer, originally designed as an editing computer, was named BOGART after the city editor of the New York SUN. The name ROB ROY was not an acronym, but popular ingenuity explained it as one: "Remotely Operated BOGART--Remotely Operated by You."

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

The outstation looked like a modified government gray desk. Paper tape was output through a hole in the bottom righthand drawer, and hard copy was produced off-line by reading the paper tape through a Flexwriter. I counted about 80 general and special-purpose programs in a ROB ROY manual I came across recently, many of them with familiar names like BAYOU, HUSK, STET, and DIANA.

In 1963, ROB ROY was replaced by RYE.<sup>4</sup> The extent to which analysts had come to depend on doing their cryptanalysis by computer can be measured by the large number of programs--now for the first time called "GUPPIES"--programmed for the new remotely-operated system, and by the numerous outstations used. At present, RYE outstations number more than 150. Indeed, the demands for service have at times outweighed RYE's ability to fill them. As a result, many GUPPY programs have been rewritten for other computers, notably for DCS,<sup>5</sup> starting in 1966.

From very early, and increasingly as time went on, the cryptanalyst programmers designed their programs to be both "General" and "Utility."

The "Utility" portion of the GUPPY name stems from the fact that many of these programs are computerized versions of the day-to-day standard cryptanalytic tasks performed all over the Agency. Some in fact were, and are, versions of pre-computer specialized equipment, like GEEWHIZZER which was originally the name of an Electro-Mechanagrammer. All cryptanalysts, whether they work manual or machine cryptosystems, are generally concerned with substitution, transposition, or some combination of the two. And all cryptanalysts need worksheets, frequency counts, statistics, decrypts, and indexes; they need to drag cribs and to test keys in order to do their jobs. These are like electricity and water "utilities" to the cryptanalysts, and many are handled by the GUPPY programs.

Flexible parameters make the GUPPY programs "General." One cryptosystem differs from another primarily in the crypto-variables (figures, cipher alphabets, and keys) associated with it, its character set, and the underlying language. Most GUPPIES are not limited either in the kind of data they accept or the way they handle it. Almost all of them contain a generalized parameter-handler routine that allows the user to tailor a program to his specific needs.

4. RYE is not an acronym. Two computers--UNIVAC 490 and UNIVAC 494--have been used on this system.

5. Direct-Coupled System, using IBM hardware.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

For example, the GUPPY programs will accept a character set 2 through 64 long; data can be prepared on paper tape or cards, or on a variety of equipment (ASR-35, CXCO, FLEX). Options abound for specifying arithmetic (additive, subtractive, minuend, Baudot), widths, graph sizes, sort fields, and data arrangement. Thresholds can often be changed, specialized log weights input, and instructions for formatting of printout given.

Descriptions of the GUPPY programs are published in the GUPPY Manuel available from Mrs. Linda Sweeney, C4, phone 3829s. This publication is available to any interested cryptanalyst. In addition, the use of RYE and of the GUPPY programs is taught in three courses conducted by the Cryptanalysis Department of the NCSch. They are: General Cryptanalysis (CA-100), Practical Diagnosis (CA-260), and Rye Operations for Cryptanalytic Applications (CA-090). The latter course is a new one; the pilot class was held in March 1973.

In G Group, Mr. J. D. Tankersley is always available to give assistance on RYE both to cryptanalysts and to open-shoppers. In his office, 3A111 (phone 4727s), he maintains a file of all the GUPPY program assemblies and a library of punched paper tapes of plain text and weights for some of the G Group languages. He also serves as GUPPY trouble shooter and is the person to call if a program seems to be in trouble.

Instructors in the Cryptanalysis Department are also glad to assist cryptanalysts in using RYE in any way they can. The phone number of 8025/36; the room number in FANX II is A2A32B.

\* \* \* \*

TRANSLATION, PLEASE?

SAVILLE DER DAGO  
TOUSEND BUZES IN ARO  
NOCHOE DEM IST TROUXS  
SUMMIT COUZIN  
SUMMIT DOUXS

Vince Las Casas, B6



(See answer on page 28)

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~An Alphabetical Guide to the GUPPIES

- \* [PROGRAMS WHICH PUNCH TAPES AS WELL AS PRINT ARE MARKED WITH AN ASTERISK.] \*
- + [BAUDOT PROGRAMS OR ONES WITH BAUDOT OPTIONS ARE MARKED WITH A PLUS SIGN.] +
- ASKIT: Predicts or evaluates results of polyalphabetic depth search based on Kappa test.
- +BALK: Prints worksheet, 3 to 100 characters per line.
- \*BAYOU: Prints monographic and digraphic frequency counts, log and category weights for chained, disjointed or transposition digraphs.
- +\*BDELT: Makes Baudot horizontal or intermessage difference streams.
- +BEE: Prints binary 5-level differences and statistics.
- BIGSTET: Standard diagnostic STET tests on option, some with thresholds, but handles more data, widths, intervals and prints columnar counts.
- BISEC: Key recovery and decryption via generatrices and scores, for monoalphabetic in fixed-length-section cipher.
- BREN: Route and grille transposition decrypt, span < 450.
- +BUNK: Key drag and difference stream, Baudot arithmetic.
- CALC: Desk calculator functions: +, -, x, ÷, exponentiation, square root, number base change.
- CASANOVA: Periodic polyalphabetic intermessage depth search, individual or all monographic column pairs on a width.
- CHICKADEE: Diagnoses and exploits stagger bust.
- COLLEEN: Mono-, di-, and trigraphic columnar counts and statistics on a width.
- COPPERHEAD: Polyalphabetic polygraphic depth search.
- CRAZYQUILT: Transposition bust exploitation.
- CROSSUM: Cross-product sums and repeat rates at all slides for all pairs of N frequency distributions.
- DELPHI: Key recovery and decryption, periodic polyalphabetic, related or unrelated alphabets.
- +\*DELT: Horizontal or intermessage differences or sums, modular or Baudot arithmetic.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~+\*DELTBDELT:   


DIANA: Digraphic counts and statistics.

\*DOBE: Unilateral (1 for 1) substitution decrypt or conversion.

\*DOBE2: Biliteral (2 for 1) substitution decrypt or conversion.

DOODLE: Formatted worksheets, specified hits underlined. Hat and crenelated diagrams.

+DOPE SHEET: Probabilistic worksheet for polyalphabetic depth reading.

EPICTETUS: Enciphered indicator search.

+FINKSBURG: Diagnostics on levels of 5-level streams.

FLUSH: Aperiodic polyalphabetic depth search.

FREQWIDTH: Prints formatted worksheet, with count below each group.

GEEWHIZZER: Anagrams columnar and grille transposition.

+\*GEORGE: General purpose encipher/decipher of transposition, monoalphabetic and polyalphabetic substitution and Hagelin. Related or unrelated alphabets.

+\*GIMP: Polyalphabetic crib drag.

GROUPDATA: Prints formatted worksheets.

+HUSH PUPPY: Polyalphabetic crib and key drag. Monographic log weights.

INDEX: Index and frequency counts, user-specified sort order.

ISOM: Locates isomorphs.

JEZEBEL: Decrypts biliteral substitution. Coordinates may be summed, with variants, or appear nonconsecutively in cipher.

KRAKUP: Tests for cyclic phenomena in nonhomogeneous material.

KYOTO: Tests and exploits stagger bust situation in polyalphabetics.

\*LACER: Interlaces 2 data streams to user specification.

LAMBRØS: Key recovery and decryption via generatrices and scores for periodic polyalphabetic.

LILINDEX: Index and frequency counts, user-specified sort order, limited amount of data.

+LOGDIFF: Computes monographic plain and theoretical difference log weights.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

MARTEE: Recovers key length for monoalphabetic-in-fixed-length encipherment.

+\*MASK: Deletes characters or levels on cycling basis.

MODIRA: Coordinate recovery for monomedinome.

MONDIN: Prints monome-dinome worksheets and decrypts.

+MONDITRI: Mono-, di-, and trigraphic frequency counts of selected levels and level combinations.

MONOSEC: Replaces MARTEE (same options).

MYSTARS: Sorts 2-5 character groups from 1 stream; differences and sorts differences from 2 streams.

\*NEPTUNE: Decrypts transposition within span of 100.

OVERLAP: [Redacted]

PASDEDEUX: [Redacted]

+PICKWICK: Theoretical cipher distribution and log weights for polyalphabetic.

POLLY: Lists overall and oncut polygraphic repeats. Statistics.

PROFILE: Displays trilateral frequency distribution a la MC-I, pg. 72.

PUSHUP: Tests polyalphabetic depths and prints depth reader's worksheet.

QUIKROB: Polyalphabetic depth test, modified Kappa scoring on limited data.

QUIKSTET: SFET on limited data.

QUIKTWIST: TWIST on limited data.

QUIKWHIZ: GEEWHIZZER on limited data.

QUIKXIBAR: XIBAR on limited data. No frequency counts option.

RITWIDTH: General purpose worksheet preparation, user specifications.

ROBIN: Polyalphabetic depth search.

ROLLFAST: Generatrices for 1 stream or pairs of 2 or 3 streams, formatted output.

RUMDUM: Sorts message identification streams prepared for INDEX.

SALLY: Prints monome-dinome frequency count.

+SCOOT: Polyalphabetic crib and key drag. Tetragraphic weights and cribs from TAPIR.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

SHADOW: Profile monographic frequency count on data and on horizontal delta. Statistics.

SMARTSET: STET plus chi-square; threshold option.

STET: Prints standard diagnostic statistics and counts.

STUBBY: Remainder test.

+SUMDIF:

SYLLABLE: General purpose matrix decrypt (up to 36x36), plain and cipher unit sizes 1-5.

SYNDROME: Coordinate recovery, worksheets, frequency counts and decryption for monome-dinome.

TABLES: Tailor-made mathematical tables: chi-square and binomial probabilities; prime factors and numbers; combinations N things r at time; transposition column factors and matrix widths.

TAPECON: Produces hard copy from paper tape, acting on functions.

+\*TAPIR: Alphabetic, inverse frequency lists and log weights for 3, 4, 5 character groups.

TASKAN: Single, double transposition key test.

THUD: Makes depth reader's worksheet.

TREES: General purpose book-breaker's package: counts, indexes, WMP's, codebooks, et al.

TWIST: Single, double transposition decrypt.

UNICORN: Stripped-down version of SHADOW.

\*UNLACER: Creates 2 data streams from 1 according to user specifications.

+\*VIGORO: Creates streams of X's and O's from 5 or 6 level tape.

+WARP: Difference or decrypt polyalphabetic substitution.

+WENDY: Prints binary worksheet (X's and O's) from 5 level characters.

WIDTH: Prints frequency counts and statistics for columns of width write-out.

XIBAR: Makes frequency counts overall on individual messages or on columns of width and subdivides them into homogeneous sets.

\*XPAN: Creates data stream expanded positionally by specified characters.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~A Categorical Guide to the GUPPIES

<u>Anagram</u>	<u>Bookbreaking</u>	TAPECON UNLACER VIGORO XPAN
GEEWHIZZER QUIKWHIZ	FREQWIDTH GOUPDATA INDEX LILINDEX POLLY RITWIDTH TAPIR TREES	<u>Decryption for Substitution</u>
<u>Baudot</u>	<u>Bust Exploitation</u>	BISEC DELPHI DELT DELTDELTA DOBE DOBE2 GEORGE JEZEBEL LAMBROS MONDIN SYLLABLE TREES WARP
BALK BDELT BEE BUNK DELTDELTA DOPESHEET FINKSBURG GEORGE GIMP HUSHPUDDY LOGDIFF MASK MONDITRI PICKWICK SCOOT SUMDIF TAPIR VIGORO WARP WENDY	CHICKADEE CRAZYQUILT KYOTO	<u>Decryption for Transposition</u>
	<u>Chi-Square</u>	BREN GEORGE NEPTUNE QUIKTWIST TWIST
	FINKSBURG SMARTSTET TABLES	
	<u>Conversion</u>	
	See Decryption	
	<u>Crenelated Diagram</u>	
<u>Binary</u>	DOODLE	<u>Depth Test</u>
BEE FINKSBURG MASK MONDITRI VIGORO WENDY	<u>Crib/Key Drag</u>	ASKIT CASANOVA COPPERHEAD CROSSUM FLUSH PUSHUP QUIKROB ROBIN
	BUNK GIMP HUSHPUDDY SCOOT	
<u>Binomial</u>	<u>Data Processing</u>	<u>Desk Calculator</u>
TABLES	BALK LACER MASK ROLLFAST (Cont'd in next column)	CALC

~~TOP SECRET UMBRA~~Differences

BDELTA  
BEE  
BUNK  
DELTA  
DELTABDELTA  
MYSTARS  
OVERLAP  
ROLLFAST  
SHADOW  
SUMDIF  
WARP

Frequency Counts

BAYOU  
BIGSTET  
COLLEEN  
DIANA  
FREQWIDTH  
INDEX  
LILINDEX  
MONDIN  
MONDITRI  
PROFILE  
QUIKSTET  
QUIKZIBAR  
SALLY  
SHADOW  
SYNDROME  
TAPIR  
UNICORN  
WIDTH  
XIBAR

Frequency Profiles

PROFILE  
SHADOW  
UNICORN

Generatrices

BISEC  
LAMBROX  
ROLLFAST

Hat Diagram

DOODLE

Homogeneity

BIGSTET  
QUIKSTET  
QUIKXIBAR  
STET  
XIBAR

I.C. and/or Sigmage

ASKIT  
BEE  
BIGSTET  
CASANOVA  
COLLEEN  
CROSSUM  
DELTA  
DELTABDELTA  
DIANA  
EPICTETUS  
GDELTA  
KRAKUP  
MARTEE  
MONOSEC  
MYSTARS  
PASDEDEUX  
POLLY  
PUSHUP  
QUIKSTET

QUIKXIBAR  
SHADOW  
SMARTSTET  
STET  
TAPIR  
UNICORN  
WIDTH  
XIBAR

Index

INDEX  
LILINDEX

Indicators

EPICTETUS  
INDEX  
MYSTARS  
RUMDUM  
SUMDIF

Inverse Frequency

TAPIR  
TREES

Isomorphs

ISOM

Key/Alphabet Test

BISEC  
DELPHI  
DOPE SHEET  
LAMBRØS  
TASKAN

Local Roughness

BIGSTET  
MARTEE  
MONOSEC  
QUIKSTET  
SMARTSTET  
STET



~~TOP SECRET UMBRA~~Log WeightsBAYOU  
LOGDIFF  
PICKWICK  
TAPIRMath Tables

TABLES

Matrix Factors/  
Dimensions

TABLES

DELTDDELTD  
OVERLAP  
SUMDIFMonome-To-Dinome  
Ratio

MODIRA

Polygraphic RepeatsBIGSTET  
COLLEEN  
COPPERHEAD  
DOODLE  
INDEX  
LILINDEX  
MYSTARS  
OVERLAP  
POLLY  
QUIKSTET  
STET  
SUMDIF  
TAPIRPrime Factors/  
Numbers

TABLES

Probability  
Tables

TABLES

Remainder Test

STUBBY

Repeat RateCOLLEEN  
CROSSUM  
DIANA  
KRAKUP  
SYNDROME  
TAPIR  
UNICORNSortsINDEX  
LILINDEX  
MYSTARS  
OVERLAP  
SUMDIF  
TAPIRStatisticsSee Chi-Square,  
I.C. Sigmage,  
Log Weights  
Repeat RateStub Test

STUBBY

Theoretical CipherLOGDIFF  
PICKWICKVariantsBIGSTET  
GEORGE  
INDEX  
QUIKSTET  
STET  
SYLLABLEWidthsBIGSTET  
CASANOVA  
COLLEEN  
CROSSUM  
DOODLE  
KRAKUP  
LAMBROS  
OVERLAP  
PASDEDEUX  
QUIKSTET  
SMARTSTET  
STET  
WIDTH  
XIBARWorksheetsDOODLE  
FREQWIDTH  
GROUPDATA  
MONDIN  
PUSHUP  
RITWIDTH  
SYNDROME  
THUD  
WENDY~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~Cryptosystem Guide to the GUPPIES

Following is a list of the cryptosystems covered in this Guide:

1. MONOALPHABETIC SUBSTITUTION -  
Unilateral; bilateral; monome-dinome; matrix (bipartite, digraphic); code.
2. PERIODIC POLYALPHABETIC AND CYCLIC ADDITIVE SUBSTITUTION.
3. APERIODIC POLYALPHABETIC AND NONCYCLIC ADDITIVE SUBSTITUTION -  
General; Baudot; binary; ciphertext autokey; Hagelin; monoalphabetic in fixed-length section; progressive.
4. TRANSPOSITION -  
General; bisection, railfence; columnar (single, double); grille, local, route; transposed code.
5. PLAINTEXT PROCESSING

<u>UNILITERAL</u>	<u>FREQUENCY PROFILES</u>	<u>INDEX, SORTS</u>
<u>CHI-SQUARE</u>	FREQWIDTH	INDEX
<u>SMARTSET</u>	INDEX	LILINDEX
<u>TABLES</u>	LILINDEX	
	QUIKXIBAR	<u>KEY/ALPHABET TEST</u>
<u>DECRYPTION</u>	STETs	LAMBROS
DOBE	XIBAR	
GEORGE		<u>NULLS, MASKS</u>
LAMBROS	<u>HOMOGENEITY</u>	GEORGE
	CROSSUM	MASK
<u>DIAGNOSIS</u>	QUIKXIBAR	
STETs	STETs	<u>POLYGRAPHIC REPEATS</u>
	XIBAR	DOODLE
<u>DIFFERENCES</u>	<u>I.C.</u>	INDEX
DELT	DELT	LILINDEX
DELTBDELT	DELTBDELT	POLLY
ROLLFAST	POLLY	STETs
SHADOW	PUSHUP	
	QUIKXIBAR	<u>REPEAT RATE</u>
	SHADOW	CROSSUM
	STETs	UNICORN
	UNICORN	
	XIBAR	

~~TOP SECRET UMBRA~~

<u>VARIANTS</u>	<u>I.C.</u>	<u>MONOME-DINOME</u>
DOBE	BAYOU	<u>COORDINATE RECOVERY</u>
GEORGE	COLLEEN	MODIRA
INDEX	DIANA	SYNDROME
	MYSTARS	
<u>WEIGHTS</u>	STETS	
BAYOU		<u>DECRYPTION</u>
LOGDIFF		MONDIN
	<u>INDEX, SORTS</u>	SYNDROME
<u>WORKSHEETS</u>	INDEX	
DOODLE	LILINDEX	<u>DIAGNOSIS</u>
FREQWIDTH	MYSTARS	STETS
GROUPDATA		SYNDROME
PUSHUP	<u>NULLS, MASKS</u>	
RITWIDTH	DIANA	<u>DIFFERENCES</u>
THUD	MASK	DELT
		DELTBDELT
<u>BILITERAL</u>	<u>POLYGRAPHIC REPEATS</u>	
	COLLEEN	<u>FREQUENCY COUNTS</u>
<u>DECRYPTION</u>	DOODLE	MONDIN
DOBE2	INDEX	SALLY
JEZEBEL	LILINDEX	SYNDROME
SYLLABLE	MYSTARS	
	POLLY	<u>HOMOGENEITY</u>
<u>DIAGNOSIS</u>	STETS	STETS
STETS		SYNDROME
	<u>REPEAT RATE</u>	
<u>DIFFERENCES</u>	COLLEEN	
DELT	DIANA	<u>I.C.</u>
DELTBDELT		BAYOU
MYSTARS	<u>VARIANTS</u>	DELT
	DOBE2	DELTBDELT
<u>FREQUENCY COUNTS</u>	SYLLABLE	POLLY
BAYOU	JEZEBEL	STETS
COLLEEN	INDEX	
DIANA		<u>INDEX, SORTS</u>
FREQWIDTH	<u>WEIGHTS</u>	INDEX
INDEX	BAYOU	LILINDEX
LILINDEX	LOGDIFF	
		<u>MONOME-TO-DINOME</u>
<u>HOMOGENEITY</u>	<u>WORKSHEETS</u>	RATIO
DIANA	DOODLE	MODIRA
QUIKXIBAR	FREQWIDTH	
STETS	GROUPDATA	
XIBAR	RITWIDTH	

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

<u>POLYGRAPHIC REPEATS</u>	<u>HOMOGENEITY</u>	<u>VARIANTS</u>
DOODLE	DIANA	INDEX
INDEX	STETS	JEZEBEL
LILINDEX		SYLLABLE
POLLY		
STETS	<u>I.C.</u>	<u>WEIGHTS</u>
	BAYOU	BAYOU
<u>REPEAT RATE</u>	CASANOVA	TAPIR
SYNDROME	DELT	
	DELTBDELT	<u>WORKSHEETS</u>
<u>VARIANTS</u>	DIANA	DOODLE
INDEX	MYSTARS	FREQWIDTH
MONDIN	POLLY	GROUPDATA
SYNDROME	STETS	RITWIDTH
	TAPIR	
<u>WEIGHTS</u>	<u>INDEX, SORTS</u>	<u>CODE</u>
BAYOU	INDEX	CODE BOOK
LOGDIFF	LILINDEX	TREES
	MYSTARS	
<u>WORKSHEETS</u>	TAPIR	<u>DECRYPTION</u>
MONDIN		SYLLABLE
SYNDROME	<u>INVERSE FREQUENCY</u>	TREES
	TAPIR	
<u>MATRIX: BIPARTITE</u>	<u>KEY/COORDINATE TEST</u>	<u>DIAGNOSIS</u>
<u>DIGRAPHIC</u>	CASANOVA	STET
<u>DECRYPTION</u>	CROSSUM	TAPIR
DOBE2		
JEZEBEL	<u>NULLS, MASKS</u>	<u>FREQUENCY COUNTS</u>
SYLLABLE	DIANA	FREQWIDTH
	MASK	INDEX
<u>DIAGNOSIS</u>		LILINDEX
DIANA	<u>POLYGRAPHIC REPEATS</u>	TAPIR
STETS	DOODLE	TREES
TAPIR	INDEX	
	LILINDEX	<u>HOMOGENEITY</u>
<u>DIFFERENCES</u>	MYSTARS	STETS
DELT	POLLY	TAPIR
DELTBDELT	STETS	
MYSTARS	TAPIR	<u>I.C.</u>
		CASANOVA
<u>FREQUENCY COUNTS</u>	<u>REPEAT RATE</u>	MYSTARS
BAYOU	DIANA	POLLY
DIANA	TAPIR	STETS
FREQWIDTH		TAPIR
INDEX		
LILINDEX		
TAPIR		

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~INDEX, SORTS

INDEX  
LILINDEX  
TAPIR  
TREES  
(BY CODE GP.,  
MEANING,  
VALIDITY, ANY  
SPECIFIED  
GROUPS)

INVERSE FREQUENCY

TAPIR  
TREES

NULLS, MASKS

MASK

POLYGRAPHIC REPEATS

INDEX  
LILINDEX  
MYSTARS  
POLLY  
TAPIR  
TREES

POSITIONAL ROUGHNESS

CASANOVA  
STETS

REPEAT RATE

TAPIR

VARIANTS

INDEX  
STETS  
SYLLABLE

VMP

TREES

WEIGHTS

TAPIR

WORKSHEETS

FREQWIDTH  
GROUPDATA  
RITWIDTH

PERIODIC POLYALPHA-  
BETIC AND CYCLIC  
ADDITIVE

BUST EXPLOITATION  
CHICKADEE  
KYOTO

CHI-SQUARE  
SMARTSET  
TABLES

CRIB/KEY DRAG  
GIMP  
HUSHPUDDY  
SCOOT

DECRYPTION  
DELPHI  
GEORGE  
LAMBROS  
WARP

DEPTH TESTS  
CASANOVA  
CROSSUM  
FLUSH  
PUSHUP  
XIBAR  
QUIKXIBAR

DIAGNOSIS  
STETS

DIFFERENCES  
DELT  
DELTDELTA  
MYSTARS  
OVERLAP  
ROLLFAST  
SUMDIF  
WARP

FREQUENCY COUNTS

BIGSTET  
COLLEEN  
QUIKXIBAR  
WIDTH  
XIBAR

GENERATRICES

LAMBROS  
ROLLFAST

I.C.

CASANOVA  
COLLEEN  
DELT  
DELTDELTA  
MYSTARS  
OVERLAP  
POLLY  
PUSHUP  
QUIKXIBAR  
STETS  
TAPIR  
WIDTH  
XIBAR

INDEX, SORTS

INDEX  
LILINDEX

ISOMORPHS

ISOM

KEY/ALPHABET TEST

DELPHI  
LAMBROS

MATH TABLES

TABLES

DELTDELTA  
OVERLAP  
SUMDIF

~~TOP SECRET UMBRA~~

# ~~TOP SECRET UMBRA~~

POLYGRAPHIC REPEATS

COLLEEN  
DOODLE  
INDEX  
LILINDEX  
MYSTARS  
OVERLAP  
POLLY  
STETS  
SUMDIF  
TAPIR

REMAINDER/STUB TEST  
STUBBY

REPEAT RATE

COLLEEN  
CROSSUM  
TAPIR

UNRELATED CIPHER

ALPHABETS  
CASANOVA  
DELPHI  
GEORGE

WEIGHTS

BAYOU  
LOGDIFF  
TAPIR

WORKSHEETS

DOODLE  
GROUPDATA  
OVERLAP  
PUSHUP  
RITWIDTH  
THUD

APERIODIC POLYALPHA-  
BETIC AND NONCYCLIC  
ADDITIVE

BUST EXPLOITATION

CHICKADEE  
KYOTO

CHI-SQUARE

SMARTSTET  
TABLES

CRIB-KEY DRAG

GIMP  
HUSHPUDDY  
SCOTT

DECRYPTION

DELPHI  
DELT  
DELTBDELT  
GEORGE

DEPTH TESTS

ASKIT  
COPPERHEAD  
CROSSUM  
FLUSH  
PUSHUP  
QUIKROB  
ROBIN

DIAGNOSIS

STETS

DIFFERENCES

DELT  
DELTBDELT  
MYSTARS  
OVERLAP  
ROLLFAST  
SUMDIF  
WARP

FREQUENCY COUNTS

COLLEEN  
XIBAR

GENERATRICES

ROLLFAST

I.C.

ASKIT  
BAYOU  
DELT  
DELTBDELT  
MYSTARS

POLLY

PUSHUP  
QUIKXIBAR  
STETS  
TAPIR  
XIBAR

INDEX, SORTS

INDEX  
LILINDEX  
MYSTARS  
OVERLAP  
SUMDIF

INDICATORS

EPICTETUS

ISOMORPHS

ISOM

KEY/ALPHABET TEST

DOPESHEET

LOCAL ROUGHNESS

MARTEE  
MONOSEG  
STETS

MATH TABLES

TABLES

DELTBDELT

OVERLAP  
SUMDIF

POLYGRAPHIC REPEATS

COPPERHEAD  
DOODLE  
INDEX  
LILINDEX  
MYSTARS  
OVERLAP  
POLLY  
STETS

REMAINDER/STUB TEST

STUBBY

~~TOP SECRET UMBRA~~

REPEAT RATE  
CROSSUM  
OVERLAP  
TAPIR

THEORETICAL CIPHER  
LOGDIFF  
PICKWICK

WEIGHTS  
BAYOU  
LOGDIFF  
PICKWICK  
TAPIR

WORKSHEETS, OVERLAP  
DOODLE  
PUSHUP  
THUD

BAUDOT

CRIB/KEY DRAG  
BUNK  
GIMP  
HUSHUPPY  
SCOOT

DECRYPTION  
GEORGE  
WARP

DIFFERENCES  
BDELT  
BUNK  
DELTBDELT  
SUMDIF  
WARP

KEY/ALPHABET TEST  
DOPE SHEET

[Redacted]

SUMDIF

NULLS, MASKS  
MASK

THEORETICAL CIPHER  
PICKWICK

WEIGHTS  
LOGDIFF  
PICKWICK  
TAPIR

WORKSHEETS  
BALK

BINARY

CHI-SQUARE  
FINKSBURG

DATE PROCESSING  
VIGORO

DENSITY COUNTS  
FINKSBURG

DIFFERENCES  
BEE

LEVEL COUNTS  
BEE  
FINKSBURG  
MONDITRI

MASKS  
MASK

SIGMAGE  
BEE  
FINKSBURG

WORKSHEET  
WENDY

CIPHERTEXT AUTOKEY

DECRYPTION  
DELTBDELT  
GEORGE

DIAGNOSIS  
DIANA



MONOALPHABETIC IN  
FIXED-LENGTH  
SECTIONS

DECRYPTION  
BISEC

GENERATRICES  
BISEC

KEY/ALPHABET TEST  
BISEC

LOCAL ROUGHNESS  
MARTEE  
MONOSEC

PROGRESSIVE

DECRYPTION  
ROLLFAST

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~TRANSPOSITION

ANAGRAM  
GEEWHIZZER  
QUIKWHIZ

CHI-SQUARE  
SMARTSTET  
TABLES

CRELATED DIAGRAM  
DOODLE

DECRYPTION  
BREN  
GEORGE  
LACER  
NEPTUNE  
QUIKTWIST  
TWIST

DIAGNOSIS  
STETs

FREQUENCY COUNTS  
STETs

FREQUENCY PROFILES  
SHADOW  
UNICORN

HAT DIAGRAM  
DOODLE

I.C.  
POLLY  
SHADOW  
STETs  
TAPIR  
UNICORN

INDEX, SORTS  
INDEX  
LILINDEX

LOCAL ROUGHNESS  
STETs

MATRIX FACTORS/  
DIMENSIONS  
TABLES

NULLS, MASKS  
GEORGE  
MASK

POLYGRAPHIC REPEATS  
DOODLE  
POLLY  
STETs  
TAPIR

REMAINDER/STUB  
TEST  
STUBBY

REPEAT RATE  
TAPIR  
UNICORN

WEIGHTS  
BAYOU  
LOGDIFF

WORKSHEETS  
DOODLE  
FREQWIDTH  
GROUPDATA  
PUSHUP  
RITWIDTH

BISECTION, RAILFENCE

DECRYPTION  
LACER

COLUMNAR, SINGLE/  
DOUBLE

BUST EXPLOITATION  
CRAZYQUILT

DECRYPTION  
GEORGE  
QUIKTWIST  
TWIST

KEY TEST  
TASKAN

GRILLE, LOCAL, ROUTE

DECRYPTION  
BREN  
GEORGE  
NEPTUNE

TRANSPOSED CODE

DECRYPTION  
GEORGE/TREES

PLAINTEXT PROCESSING

CHI-SQUARE  
SMARTSTET

DATA PROCESSING  
LACER  
MASK  
ROLLFAST  
TAPECON  
TREES  
UNLACER  
VIGORO  
XPAN

DIFFERENCES  
DELT  
DELTBDELT  
SHADOW  
SUMDIF

ENCRYPTION  
GEORGE

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

FREQUENCY COUNTS

BAYOU  
DIANA  
INDEX  
LILINDEX  
PROFILE  
SHADOW  
STETs  
TAPIR  
TREES  
UNICORN

POLYGRAPHIC REPEATS

INDEX  
LILINDEX  
POLLY  
STETs  
TAPIR

REPEAT RATE

DIANA  
TAPIR  
UNICORN

FREQUENCY PROFILES

PROFILE  
SHADOW  
UNICORN

THEORETICAL DIFFERENCE

WEIGHTS  
BAYOU  
LOGDIFF  
PICKWICK  
TAPIR

GENERATRICES

ROLLFAST

WORKSHEETS

DOODLE  
PUSHUP  
RITWIDTH

I.C.

BAYOU  
DELT  
DELTBDELT  
DIANA  
POLLY  
SHADOW  
STETs  
TAPIR  
UNICORN

\* \* \* \*

INDEX, SORTS

INDEX  
LILINDEX  
TAPIR  
TREES

INVERSE FREQUENCY

TAPIR  
TREES



DELTBDELT  
SUMDIF



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

## Memorandum

TO : All Personnel concerned

FROM : Chief, color coordinating division

SUBJECT: File copies

It has been brought to my attention that a change in the standard color sorting scheme is necessary due to the loss of the green copies we have been receiving. The following steps will be taken to correct the situation until green copies are received again:

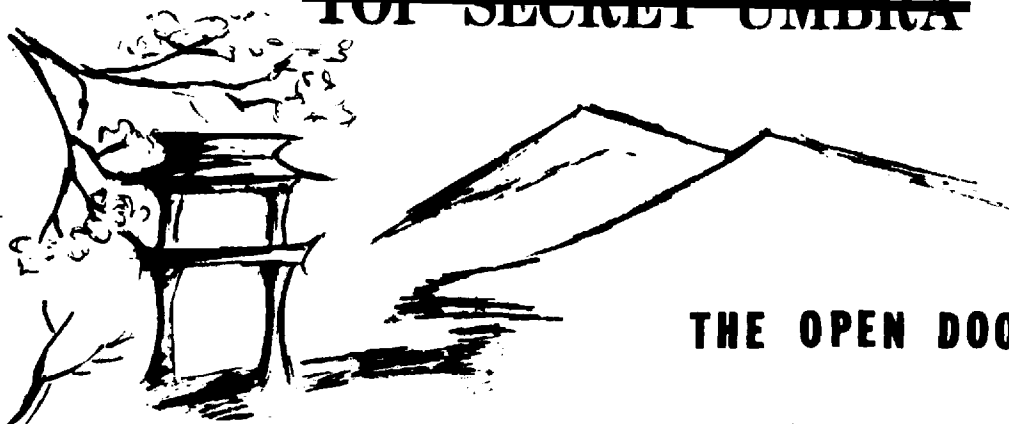
1. Blue - This copy is not received and will not be received. No change in handling is needed.
2. Green - Where green continues to be forwarded it will be filed in the green file in accordance with current procedures. This will be true at all times that green is forwarded along with yellow, pink, and gold. If forwarded without one or all of the other colors it will still be filed under green.
3. Yellow - Yellow will remain yellow and not be substituted for either green or pink. It will be held for a 30 day period and then thrown away as it is of no use at all. If it is the only copy it will be marked and placed in a special non-green file to prevent confusion.
4. Pink - Where green is not available pink will become green and be filed in the green file in lieu of green or yellow. In this case pink will NOT be thrown away. Note that pink can never be substituted for yellow.
5. Gold - If green or pink is unavailable, Gold will become green. It will be specially marked to prevent its being confused with yellow. Otherwise gold will always be thrown away.
6. White - This is not received. Handling procedures remain the same.

Please implement the above policy as appropriate.

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~



## THE OPEN DOOR

*We seek to be companions along the way.  
 The lantern which we carry is not ours.  
 The spirit which we share is contagious thought;  
 The knowledge which we gain, an illuminating torch  
 And all who seek may perceive and learn.*

-The Concept of Dragon Seeds

### A PEBBLES TO PEOPLE MESSAGE

Sally Peebles, G52, Ret.

*We all expect our COMINT targets to become increasingly secure as time passes, and what we learn from reading early systems can be invaluable in enabling us to read successor, more difficult systems.*

### Search and Destroy Missions

Periodically we must undertake to weed out material in our over-stuffed cabinets, shelves, and desks to forestall ultimate suffocation under masses of our own paper. Nobody should argue against our cleaning our own figurative Augean Stables. It is the method of accomplishing this task that concerns me, since this job, if done ruthlessly and without informed discrimination, can seriously impair or even preclude future successes.

### Youth Is Not Necessarily Beauty, Nor Beauty Youth

When the order to clean out is given, some enthusiasts zestfully fill burn bags and bulk burn boxes with anything non-current at hand in which they personally have no interest. This clean-sweep attitude promotes a feeling of accomplishment and virtue, since it makes room for new stuff and shows the boss that you are cooperating fully! However, the reckoning may come much later when the spree of "throwing out the baby with the bath water" causes analysts to waste hours, day - even months - searching for missing material, or trying to rebuild records which have been thoughtlessly destroyed.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Haven't you heard, "Whatever became of that ZEM personality file we used to have two reorganizations ago?" or, "We used to read a ZEA system. Don't we have any language patterns, any key studies, frequencies, or samples of decrypted traffic? How did that old system work?" (Have you ever tried to figure out how a system worked with no documentation except a Master File Sheet?).

One Man's Litter Is Another Man's Dead Sea Scrolls

Not too long ago I had cause to wail because somebody made a unilateral decision and threw away a precious, somewhat elderly, telephone directory which we treasured because it contained complete and explicit Order of Battle information *in clear and in Spanish!* Time after time this yielded answers which we could find nowhere else. (The target government got smarter after that, so that subsequent directories contained less helpful information.)

A similar invaluable, unique antique has a happier fate. This 1962 OB document I have worn thin but managed to preserve because I never let it stray from my possession. No other document provides such complete information, and *in Spanish*. (All too often we may know only the meaning or English translation of something without knowing how our special target expresses it in his own idiom.)

As for traffic, sometimes vintage traffic may be far more useful than recent stuff. Quality copy from happier days may get you farther faster than quantities of current slush even if some intervening changes in the system have been made. We all expect our COMINT targets to become increasingly secure as time passes, but what we learn from reading early systems can be invaluable in enabling us to read more difficult successor systems, whether the difficulty stems from sophistication or from the miserable quality of recent intercept.

But suppose the quality and quantity of traffic are not in question. It still is a general verity that early systems are less secure than later ones. Therefore it is wasteful and foolhardy not to squeeze as much long-term information as possible from the decryptions of early systems: the usual statistics, common beginnings and endings, characteristic expressions, etc. I never cease to be astonished at how *unlike* one another are the speech habits of different services

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

of the same country, let along those of different countries, even though in all cases the language is Spanish. There simply is no substitute for knowing how each entity talks. So, both for now and for the future, get machine runs which can be readily manipulated to provide appropriate data on each target and see that these vital statistics are preserved and used. You can't count on maintaining continuity thanks to a goof which provides you with a golden compromise. That will be the message that didn't get intercepted!

And don't forget the treasures which may be found in plain text. The P/T reference to an encrypted message may provide you with a valuable clue to the context of the referenced message. "Think on these things" - preferably before the deadline day when your fat storage areas must lose all those pounds and reason is supplanted by muscle.

#### Some Suggestions and Exhortations

1. Don't entrust the "riffing" of overweight files to someone who has a limited specialty and a compartmented mind. Since some material is important for several related specialties, a person with broad experience and a long-range viewpoint should supervise destruction parties. When in doubt about the value of keeping something, don't be timid about asking knowledgeable experts to help make decisions.

2. Often there are several copies of the same material. Perhaps all but one copy, designated "Record Copy," can be thrown out. Make sure that the Record Copy is made available to all those who need it and who *return* it.

3. See if some bulky materials can't be reduced in size. That late lamented telephone directory I referred to could have been thrown away without a regret if I had first been given the opportunity to tear out and preserve about a dozen vital pages.

4. Perhaps in the future, some large machine runs could be printed on the new IBM "compact printing device" described in the December 1970 Keyword article "Train's In!" This could vastly reduce the storage space required for runs which should be retained for a long time.

5. What is the possibility of microfilming records which should be kept indefinitely for historical reasons but which are not used frequently?

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

6. How about converting that relatively static information now on cards in a bulky file box into a 2- or 3-page printed working aid?

7. I propose the consideration of creating a central crypt and T/A repository something like our G54 C/L library. Since NSA is so prone to organize and reorganize frequently and since personnel changes at all levels almost if not completely eliminate continuity, a repository for useful references, documentation, records, etc., would eliminate the necessity for duplicate copies in several organizational segments. This plan might overcome confusion and losses of background information caused by realigning entities like ZED, ZEA, ZEN, etc., which at one time were all in the same organization but later were separated: ZED in one division, the other ZE systems in another division. (Probably they will all be reunited in some future reorganization.)

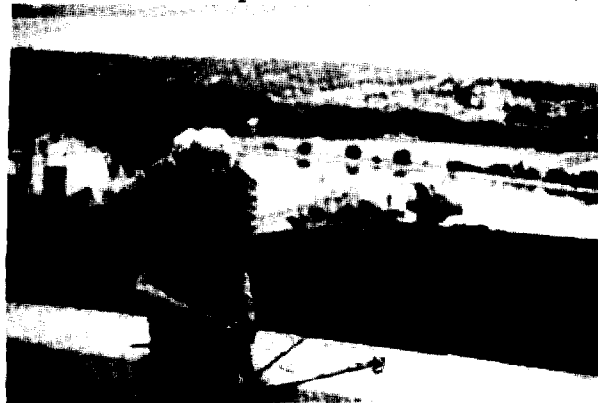
8. Everybody will hate me for this final suggestion because it involves just another tedious chore to do. However, since I'm about to leave the Agency, maybe I can get away before the Furies catch me.

When I was preparing some records as a legacy for any successor working on a particular system, I decided it would help to list the records vital to the system and the records or materials which are useful but of secondary importance. Such lists on all systems would help those who must decide what goes OUT in a pinch for space, and what must be kept or cogitated over before keeping or destroying.

In that repository, which I proposed, a single retention copy of Vital Records on non-current systems could be kept available for reference by everybody interested -- irrespective of current, past, or future organizational designations.

And now please excuse me. I really must slip out quickly . . .

(Reprint from *KEYWORD*, February 1971)

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~B SIGNALS LAB CAPABILITIES AND MISSION

by Robert Earles, B43

Up until November 1973 the B4 signals lab was referred to as the "CYANIDE" lab. This label was certainly warranted because 80-90 percent of the work being done at that time was associated with the processing and analysis of CYANIDE material. However, since November we have greatly expanded our lab capabilities and our workload has grown commensurately. In fact, CYANIDE now comprises less than 5% of the analysis done in the lab.

With the equipment added to the lab during the past few months, we analyze, identify, and provide limited processing for signals which fall into any of the following categories: frequency division multiplex (FDM), pulse position modulation (PPM), phase shift keying (PSK), frequency shift keying (FSK), double frequency shift (DFS), and on-off keying (OOK). In addition, we can handle single channel, multichannel and multitone transmissions and process wideband tapes (7 or 14 track) with servo function.

The signals lab is here to provide a service to B, but we can provide that service only if each element is aware of why we are here and what we can do. If you now have, or expect to have in the future, any material which requires signals analysis and/or processing, let us know and we will provide you with meaningful results as fast as possible.

For further information concerning the capabilities of the B4 signals lab and its equipment, please call Mr. Robert Earles, B43, extension 5751, Room 7A197.

\* \* \* \*

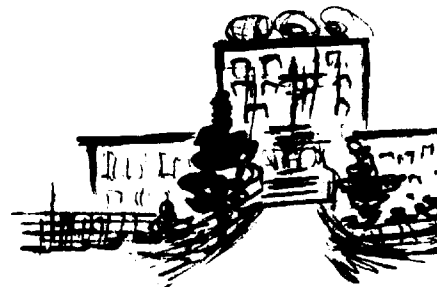
### China Buying Heavily in U.S.

**MEMPHIS (AP) — China will buy about \$1 billion worth of feed grains, soybeans and cotton in the United States this year, according to Dr. Willard Sparks, executive vice president of Cook Industries, Inc**

**He said China would buy about 140 million bushels each of wheat and corn, about 900,000 tons of soybeans and about 830,000 bales of cotton.**

Washington STAR-NEWS,  
February 1974

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~**RETURN OF.....**

Practically every spare moment during the last week of January was spent preparing for our move from Friendship to Fort Meade. We managed to keep the product flowing despite severe disruptions such as the timely cessation of DDP and ADP support at Friendship which occurred three days prior to our move, concurrent with the B11 move of 25 January. Our gear was moved from Friendship on the evening of 28 January and expertly installed by the movers. We spent the next two days putting things where they belonged, when we were lucky enough to find them.

During the week, we used one million yards of masking and other types of tape, seventeen thousand boxes of all sizes, and one marking pencil. In addition, modest estimates for the division are that we consumed over nine hundred martinis. We entertained at least twenty logistics and security staff officers from every organizational level, and we were gracious even though they only talked among themselves. We sympathized with them in their inability to assist us with the actual manual labor since (1) they wore their good clothes; (2) most had never been SIGINT analysts, hence their time was more valuable than ours; and (3) they were enroute to a B4TDLA lecture entitled "How Chinese Children Learn to Eat with Forks."

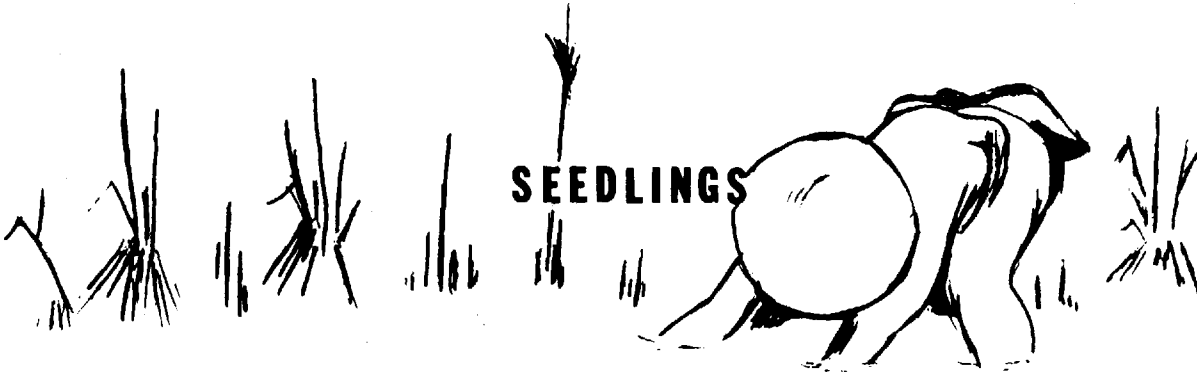
Our office is located on the fifth floor of Operations Building #1, about 50 paces from where we were located in May 1972 prior to our exodus to Friendship. We have gained much in this latest move, but we lost the blonde in E02/FANX II and the thousands of female A Group workers who wear brow shades and who, as young ladies, danced in the courts of the Ottoman Empire until their ankles swelled. We're glad to be back and invite you to visit us, but please be careful of dangling phone plugs and electrical outlets.

**....THE EXILES**

LICAMELI  
25

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~---SD 4060 COM UPGRADE

The SD4060 COM system is scheduled for an upgrade to a SD4060 system in FY 1974. The present SD4060 system has been in use at the Agency since the late 1960's, when it replaced the original SC4020 COM system. The 4060 has proved to be a dependable means of producing textual data from magnetic tape at a high rate of speed, and of reducing large volumes of intelligence to a usable form in a fraction of the amount of space required for paper output. Through its graphic capabilities the 4060 has also enabled its users to create numerous charts and graphs as another form of computer output. The system has also supported applications in the printing of various foreign languages and in scientific studies, such as random number generators.

Output from all of these applications is now recorded on 16mm roll film only. This is one of the faults of the system, for the familiar roll of microfilm can be cumbersome in many applications, and none of the data can be printed on paper with any reasonable degree of quality. With the upgrade of the SD4060, all of the systems present capabilities are retained and the output capabilities are

increased. There will be a choice of producing an image on 16mm roll film in either a 24x or 48x reduction ratio, on 35mm roll film at a 13x reduction, or on 105mm microfiche at either 24x or 48x reduction. The 35mm roll film can be used to produce aperture card inserts, projection slides, or offset plates for printing.

The microfiche capability on the COM unit provides the necessary link between the computer and the reproduction facilities and makes it possible to automatically create and update microfiche documents for mass distribution. The new and more flexible COM system will provide microforms suitable for almost any application. Acceptance of information in a "not no new" physical form will be the key to effective use of the SD4460 as it was with its predecessors.

For additional information about this forthcoming system, contact Albert J. Herb, C741,

\*\*\*\*

---CA WRITTEN EXAMINATION

The fifteenth professional qualification examination in cryptanalysis will be given on Monday and Tuesday, 13 and 14 May 1974.

All persons who took prior examinations are eligible to

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

take the May examination. To determine the eligibility of other candidates it is necessary that a copy of their Professional Qualification Record (PQR) be available to the CACP office by 19 April 1974. Although a PQR may have been submitted to M331, each aspirant should check with the CACP office to make sure that a copy of his PQR has been received by that office.

All persons who wish to take any or all of the three parts of the Examination (CA Objective, Related Fields, Essay) should notify the CACP office, Room 3C051-6, 3868sm by 26 April 1974. Each person will be notified by the CACP office of the time and place of the examination.

\*\*\*\*

---TWO ADDITIONAL SESSIONS OF:  
THE WORKSHOP IN THEORY AND  
PRACTICE OF TRANSLATION (LG-230)

This workshop is designed to provide: a) intermediate translation training, comparable to the 200-level courses in Russian, Spanish, etc., in "low-density" languages where such courses cannot be offered presently; and/or: b) additional training for persons who have taken a 200-level course and desire to further refine their translation skills or for persons in a supervisory capacity desiring to become

conversant with emerging concepts in the area of translation and evaluating translations.

INSTRUCTOR: Cpt. James J.  
Hessinger

DATES: LG-230/2/74 - 22 April-  
3 July; Monday and  
Wednesday, 8:15-  
10:15

LG-230/3/74 - 14 June-  
15 August; Tuesday  
and Thursday, 8:15-  
10:15

LOCATION: To be announced

Enrollment in each session will be limited to between six and eight students. Preference will be given to nominees who desire training in the "low-density" languages mentioned above, and who are currently assigned to duties requiring end-product translation, preliminary translation, reporting or analysis based on foreign-language source material. Nominees who do not meet both of these criteria will be considered as space permits.

Prospective students should submit NSA form 7687b, NCSch Course Application, to the element training coordinator. Nominations must be submitted on NSA form 7687 to the Language Department

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

(E11), Rm A2a26, FANX II, no later than 4 April 1974 (for LG-230/a) or 3 June 1974 (for LG-230/3).

Any prospective student should contact Cpt. Hessinger (796-6392/8027s) at the same time as he/she submits the Course Application, in order to notify him of the language in which training is desired and to permit the gathering of materials to be used in the course. A detailed description of the background, purposes and form of this workshop is available on request from the Language Department or from Cpt. Hessinger.

\*\*\*\*

ANSWER TO "TRANSLATION, PLEASE?"

SAY WILLY! THERE THEY GO.  
THOUSAND BUSES IN A ROW.  
NO JOE. THEM IS TRUCKS.  
SOME WITH COWS 'N  
SOME WITH DUCKS.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605



ASK  
THE  
DRAGON  
LADY

Dear Dragon Lady,

I read Russ Mvers' article, [redacted] in the last issue of DRAGON SEEDS. I found it interesting and am glad to see that B is beginning to be aware of the Bookbreaker's Package, thanks to you and Russ.

I found one small problem involving the terms "Decoded Index" and "Bookbreaker's Index." I'd like to suggest:

1. For "standard bookbreaker's index", substitute "standard code index (or, if there are any recoveries, a decoded index - showing the meaning on the information line for each recovered code group on major control)".

2. For "a Decoded Bookbreaker's Index", simply omit the word "Decoded", which is redundant.

Apropos - end of paragraph 2 - after messages are in case/date order do you assign a worksheet # to keep each message unique? If not, how do you solve that problem?

Keep writing; I wish others would do the same.

Kay Swift, G54, Ret.

\* \* \* \*

*May my eyes look always inward to  
the source of all my faults!*

*And, to resolve any confusion  
witnessed upon the unenlightened,  
copies of "Definitions of Bookbreaking  
Terms" are available from the Technical  
Directorates of Language and Cryptanalysis.*

*---Dragon Lady*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

## CONTRIBUTORS

BOB EARLES, B43, came to NSA as an Engineering Technician in 1960 after a three-year tour in the Army Security Agency where he served as a Cryptanalyst. He has been involved in Signals Analysis most of his Agency career and has worked in both B and G Groups. [REDACTED] Mr. Earles served as an Engineering Specialist [REDACTED] He holds professional certification in Signal Collection and Signal Conversion and has completed 24 Agency-sponsored courses in signal analysis, engineering, and management. He presently has the responsibility of supervising the personnel and job functions within the B Group Signals Analysis Lab, located in B43.

VIRGINIA JENKINS, E13, who holds an MA in Romance Languages from Duke University, has worked at NSA as a Linguist, Cryptanalyst, and Data Systems Analyst. Most recently she has been instructing and developing cryptanalysis courses in the National Cryptologic School where she is currently Head of the Cryptanalysis Department, E13. She is a member of the Cryptanalysis Career Panel, an officer in CMI, and a recipient of the Meritorious Civilian Service Award.

SALLY PEEBLES, G Group Linguist and Cryptanalyst, retired in 1971 after a long NSA career involving in turn the Middle East, the Far East, and South America. Sally was born and reared in Boulder, Colorado. At the University of Colorado, she studied English Literature, French, and Spanish and received the BA and MA as well as a fellowship to teach conversational English at the girls' normal school at Le Puy, France. She spent one summer at the University of Mexico. Since her retirement, Sally has traveled a bit and has actively supported the work and goals of the Volunteers for the Visually Handicapped of Chevy Chase, an organization which helps the blind and visually impaired to cope with their problems. She is pursuing her own goal: to live as independently and as actively as possible.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~INDEX OF PREVIOUS DRAGON SEEDS ARTICLES

(BY AUTHOR)

<u>Author</u>	<u>Article</u>	<u>Issue</u>	<u>Page</u>
ABBOTT, Walter D.	CINCPAC Intelligence Coordination Group	Vol 1, Nr 5 (Dec 72)	16
ABBOTT, Walter D.	Marketing Our Product	Vol 2, Nr 2 (Jun 73)	18
ATKINSON, Rich	Teacher Very Funny	Vol 2, Nr 3 (Sep 73)	19
BARNHILL, Peggy	AG-22 and You	Vol 1, Nr 1 (Dec 71)	9
BRANSTAD, Marti	Probing a New Technique	Vol 2, Nr 2 (Jun 73)	45
BUCK, Stuart H.	Computer-aided Bookbreaking (Not "Bookbreaking by Computer")	Vol 2, Nr 3 (Sep 73)	1
BUCKLEY, Dan	Ground Zero Approach to Language Analysis	Vol 2, Nr 1 (Mar 73)	12
CHUN, Richard S.	Need for a Centralized Transcription Operation	Vol 1, Nr 3 (Jun 72)	17
CHUN, Richard S.	Gist of the Korean SIGINT Problem	Vol 2, Nr 1 (Mar 73)	12
COURY, Sam	Surveying [REDACTED] Cryptosystems	Vol 2, Nr 3 (Sep 73)	24
CURTIN, Dick	Analyzation of Data	Vol 1, Nr 1 (Dec 71)	19
DELONG, Don	History of a Dragon	Vol 2, Nr 3 (Sep 73)	29
D'IMPERIO, Mary	CAMINO	Vol 1, Nr 2 (Mar 72)	15

EO 3.3b(3)  
PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

<u>Author</u>	<u>Article</u>	<u>Issue</u>	<u>Page</u>
DUNN, Jane E.	Once More the TSR	Vol 2,Nr 1 (Mar 73)	29
DUNN, Jane E.	SAWTOOTH Answers the Q Question	Vol 2,Nr 3 (Sep 73)	8
FERGUSON, Morris L.	Christmas at the School	Vol 2,Nr 4 (Dec 73)	17
FLYNN, William G.	The Jack Butcher Case	Vol 2,Nr 1 (Mar 73)	1
FORBES, Rodney	Reflections on a Non-Random Bane	Vol 2,Nr 2 (Jun 73)	33
GEGAN, Jeryl O.	What Have They Done To Our Linguists?	Vol 2, Nr 3 (Sep 73)	14
GERHARD, William	One Chance in Three	Vol 2,Nr 2 (Jun 73)	10
GILBERT, Allen	Impact of ARDF on Traffic Analysis	Vol 1,Nr 1 (Dec 71)	7
GILBERT, Allen	Importance of Being Honest	Vol 1,Nr 2 (Mar 72)	20
GILBERT, Allen	SEADEV--Mechanization for T/A	Vol 1,Nr 4 (Sep 72)	14
GLENN, Tom	Creative Translator	Vol 1,Nr 1 (Dec 71)	16
GLENN, Tom	Uncertain Origins	Vol 1,Nr 5 (Dec 72)	5
GLENN, Tom	Time to Look at People	Vol 2,Nr 4 (Dec 73)	19
GRANT, Louis C.	Don't Say MUSSO -- Say USSID	Vol 1,Nr 5 (Dec 72)	28
GUY, Herb	Maybe It's Related to the Phase of the Moon	Vol 1,Nr 3 (Jun 72)	5

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

<u>Author</u>	<u>Article</u>	<u>Issue</u>	<u>Page</u>
HRICIK, Mike	Things That Go Clank in the Night	Vol 1, Nr 4 (Sep 72)	7
HUNT, William	SIGINT Support on the Economic Front	Vol 2, Nr 1 (Mar 73)	18
JACOBS, Walter, Dr.	Are You Using Computers?	Vol 2, Nr 4 (Dec 73)	21
JOLLENSTEN, Ralph W., Dr.	Role of Mathematics in C/A	Vol 1, Nr 3 (Jun 72)	19
KENNARD, Bee	C Parallelogram or Vietnam Cover Story	Vol 2, Nr 2 (Jun 73)	22
KREINHEDER, Robert	Software Approach to Script Processing - The Why	Vol 1, Nr 4 (Sep 72)	19
LASLO, Mary Ann	<span style="border: 1px solid black; display: inline-block; width: 1em; height: 1em; vertical-align: middle;"></span> A Hitch-Hiking Cipher	Vol 2, Nr 2 (Jun 73)	38
LENAHAN, Donald	Cryptanalysis through Functional Linguistics	Vol 1, Nr 1 (Dec 71)	3
MILLER, Kenneth	Study of ZFK Message Activity	Vol 1, Nr 3 (Jun 72)	27
MILLER, Kenneth	Exploiting the Bust	Vol 2, Nr 1 (Mar 73)	25
MOLLICK, John	How Great COMINT Facts from Little Slivers Grow, or Making Russian Molehills Out of Chinese Mountains	Vol 1, Nr 2 (Mar 72)	26
MURPHY, Tim	Vietnamese Communist Tactical COMINT Operations	Vol 1, Nr 3 (Jun 72)	32
MYERS, L. St. Clair	Chinese Voice: Solu- tion to a Dilemma	Vol 1, Nr 4 (Sep 72)	17

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

<u>Author</u>	<u>Article</u>	<u>Issue</u>	<u>Page</u>
MYERS, Russ	Standardization????	Vol 2, Nr 1 (Mar 73)	33
MYERS, Russ	[REDACTED]	Vol 2, Nr 4 (Dec 73)	31
NUGENT, Michael	MFMUFS and Catnip	Vol 1, Nr 2 (Mar 72)	12
O'CONNOR, Ed	Viet Nam Odyssey, 1972-1973	Vol 2, Nr 4 (Dec 73)	8
ORR, E. E.	The Reality of Communications Changes	Vol 1, Nr 3 (Jun 72)	13
PALMER, Carolyn	RYE, an Extended Capacity Remote Access System	Vol 2, Nr 2 (Jun 73)	1
PATTERSON, George	Reflections on Crypt- analytic Accountability	Vol 1, Nr 2 (Mar 72)	2
PETERS, Bernie	RYE, an Extended Capacity Remote Access System	Vol 2, Nr 2 (Jun 73)	1
REINKE, F. John	Software Approach to Script Processing - The How	Vol 1, Nr 4 (Sep 72)	21
REMSBERG, Philip	CHICOM Development [REDACTED] and the AG-22	Vol 1, Nr 2 (Mar 72)	7
REMSBERG, Philip	AG-22: Where Do We Go Now?	Vol 1, Nr 5 (Dec 72)	22
SAWYER, E. Leigh	WADE-GILES System	Vol 1, Nr 5 (Dec 72)	35
SHARRETT, Jack	Development of COMINT Translation Course for Vietnamese Linguists	Vol 1, Nr 5 (Dec 72)	24
SMITH, Claire	Strategic Importance of Shenyang Military Region	Vol 1, Nr 2 (Mar 72)	23

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

<u>Author</u>	<u>Article</u>	<u>Issue</u>	<u>Page</u>
Staff Writers	SIGINT and Automatic Data Processing	Vol 1,Nr 4 (Sep 72)	12
STEPP, Leo	Viet Nam Odyssey, 1972-1973	Vol 2,Nr 4 (Dec 73)	8
STIVERS, Bill	B Needs Its Own Computer	Vol 2,Nr 4 (Dec 73)	24
STOFFEL, Wayne	Recovery of a Viet Communist Callsign System	Vol 1,Nr 1 (Dec 71)	5
SWANSON, Louise	Project KAY -- Or Another Kind of RYE	Vol 1,Nr 4 (Sep 72)	17
SWIFT, Charles	DDP--Dedupe, Delete and Progress	Vol 1,Nr 1 (Dec 71)	12
THOMAS, Jack L.	Chinese Communications Developments	Vol 2,Nr 4 (Dec 73)	2
TIREN, David J.	T/A -- Math Symposium Reviewed	Vol 1,Nr 5 (Dec 72)	36
WADDELL, Stanley	China-Wide Technical Specialists: A Way to Save Overseas	Vol 1, Nr 2 (Mar 72)	21
WILD, Norman	Machine Aided Trans- lation, Part 1	Vol 1,Nr 3 (Jun 72)	23
	Part 2	Vol 1,Nr 4 (Sep 72)	24
	Part 3	Vol 1,Nr 5 (Dec 72)	31
WOOD, Geoffrey	Rebels in Thailand	Vol 2,Nr 1 (Mar 73)	6
WOOD, Thomas	How about the Olds- mobile M?	Vol 2,Nr 1 (Mar 73)	32

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605INDEX OF PREVIOUS DRAGON SEEDS ARTICLES

(BY TITLE)

<u>Title</u>	<u>Author</u>	<u>Issue</u>	<u>Page</u>
<u>A</u>			
AG-22 and You, The	Peggy Barnhill	Vol 1, Nr 1 (Dec 71)	9
AG-22: Where Do We Go Now?	Philip Remsberg	Vol 1, Nr 5 (Dec 72)	22
Analyzation of Data	Dick Curtin	Vol 1, Nr 1 (Dec 71)	19
Are You Using Computers?	Dr. Walter Jacobs	Vol 2, Nr 4 (Dec 73)	21
<u>B</u>			
B Needs Its Own Computer	William H. Stivers	Vol 2, Nr 4 (Dec 73)	24
	Russ Myers	Vol 2, Nr 4 (Dec 73)	31
<u>C</u>			
CAMINO	Mary D'Imperio	Vol 1, Nr 2 (Mar 72)	15
CHICOM Development  and the AG-22	Philip Remsberg	Vol 1, Nr 2 (Mar 72)	7
China-Wide Technical Specialists: A Way To Save Overseas	Stanley Waddell	Vol 1, Nr 2 (Mar 72)	21
Chinese Communications Developments	Jack L. Thomas	Vol 2, Nr 4 (Dec 73)	2

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

<u>Title</u>	<u>Author</u>	<u>Issue</u>	<u>Page</u>
Chinese Voice: Solution to a Dilemma	L. St. Clair Myers	Vol 1, Nr 1 (Dec 71)	14
Christmas at the School	Morris L. Ferguson	Vol 2, Nr 4 (Dec 73)	17
CINCPAC Intelligence Coordination Group	Walter D. Abbott	Vol 1, Nr 5 (Dec 72)	16
Computer-Aided Book-keeping (Not "Book-keeping by Computer")	Stuart H. Buck	Vol 2, Nr 3 (Sep 73)	1
C Parallelogram or Vietnam Cover Story, The	Bee Kennard	Vol 2, Nr 2 (Jun 72)	22
Creative Translator, The	Tom Glenn	Vol 1, Nr 1	16
Cryptanalysis through Functional Linguistics	Donald Lenahan	Vol 1, Nr 1 (Dec 71)	3
	<u>D</u>		
DDP - Dedupe, Delete & Progress	Charles Swift	Vol 1, Nr 1 (Dec 71)	12
Development of COMINT Translation Course for Vietnamese Linguists	Jack Sharretts	Vol 1, Nr 5 (Dec 72)	24
Don't Say MUSSO--Say USSID	Louis C. Grant	Vol 1, Nr 5 (Dec 72)	28
	<u>EF</u>		
<span style="border: 1px solid black; display: inline-block; width: 50px; height: 15px; vertical-align: middle;"></span> A Hitch-Hiking Cipher	Mary Ann Laslo	Vol 2, Nr 2 (Jun 73)	38
Exploiting the Bust	Kenneth Miller	Vol 2, Nr 1 (Mar 73)	25

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~G

<u>Title</u>	<u>Author</u>	<u>Issue</u>	<u>Page</u>
Gist of the Korean SIGINT Problem	Richard S. Chun	Vol 2,Nr 1 (Mar 73)	12
Ground Zero Approach to Language Analysis	Dan Buckley	Vol 2,Nr 1 (Mar 73)	22

H

History of a Dragon	Don DeLong	Vol 2,Nr 3 (Sep 73)	29
How about the Oldsmobile M?	Thomas Wood	Vol 2,Nr 1 (Mar 73)	32
How Great COMINT Facts from Little Slivers Grow, or Making Russian Molehills Out of Chinese Mountains	John Mollick	Vol 1,Nr 2 (Mar 72)	26

I

Impact of ARDF on Traffic Analysis	Al Gilbert	Vol 1,Nr 1 (Dec 71)	7
Importance of Being Honest, The	Al Gilbert	Vol 1,Nr 2 (Mar 72)	20

JKL

Jack Butcher Case, The	William G. Flynn	Vol 2,Nr 1 (Mar 73)	1
------------------------	------------------	------------------------	---

M

Machine Aided Translation, Part 1	Norman Wild	Vol 1,Nr 3 (Jun 72)	23
Part 2		Vol 1,Nr 4 (Sep 72)	24
Part 3		Vol 1,Nr 5 (Dec 72)	31
Marketing Our Product	Walter D. Abbott	Vol 2,Nr 2 (Jun 73)	18
Maybe It's Related to the Phase of the Moon	Herbert S. Guy	Vol 1,Nr 3 (Jun 72)	5

~~TOP SECRET UMBRA~~

<u>Title</u>	<u>Author</u>	<u>Issue</u>	<u>Page</u>
	<u>N</u>		
Need for a Centralized Transcription Operation	Richard S. Chun	Vol 1,Nr 3 (Jun 72)	17
	<u>OPQ</u>		
Once More the TSR	Jane E. Dunn	Vol 2,Nr 1 (Mar 73)	29
One Chance in Three	William Gerhard	Vol 2,Nr 2 (Jun 73)	10
Probing a New Technique	Dr. Marti Branstad	Vol 2,Nr 2 (Jun 73)	45
Project KAY -- Or Another Kind of RYE	Louise Swanson	Vol 1,Nr 4 (Sep 72)	17
	<u>R</u>		
Reality of Communica- tions Changes	E. E. Orr	Vol 1,Nr 3 (Jun 72)	13
Rebels in Thailand	Geoffrey Wood	Vol 2,Nr 1 (Mar 73)	6
Recovery of a Viet Communist Callsign System	Wayne Stoffel	Vol 1,Nr 1 (Dec 71)	5
Reflections on a Non-Random Bane	Rodney Forbes	Vol 2,Nr 2 (Jun 73)	33
Reflections on Crypt- analytic Accountability	George Patterson	Vol 1,Nr 2 (Mar 72)	2
Role of Mathematics in C/A	Dr. Ralph W. Jollensten	Vol 1,Nr 3 (Jun 72)	19
RYE, an Extended Capacity Remote Access System	Bernie Peters/ Carolyn Palmer	Vol 2,Nr 2 (Jun 73)	1

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~EO 3.3b(3)  
PL 86-36/50 USC 3605

<u>Title</u>	<u>Author</u>	<u>Issue</u>	<u>Page</u>
SAWTOOTH Answers the Q Question	<u>S</u> Jane E. Dunn	Vol 2, Nr 3 (Sep 73)	8
SEADEV--Mechanization for T/A Development	Al Gilbert	Vol 1, Nr 4 (Sep 72)	14
SIGINT and Automatic Data Processing	Staff Writers	Vol 1, Nr 4 (Sep 72)	12
SIGINT Support on the Economic Front	William Hunt	Vol 2, Nr 1 (Mar 73)	18
Software Approach to Script Processing - The How	F. John Reinka	Vol 1, Nr 4 (Sep 72)	21
Software Approach to Script Processing - The Why	Robert Kreinheder	Vol 1, Nr 4 (Sep 72)	19
Standardization????	Russ Myers	Vol 2, Nr 1 (Mar 73)	33
Strategic Importance of Shenyang Military Region, The	Claire Smith	Vol 1, Nr 2 (Mar 72)	23
Study of ZFK Message Activity	Kenneth Miller	Vol 1, Nr 3 (Jun 72)	27
Surveying <span style="border: 1px solid black; display: inline-block; width: 100px; height: 1.2em; vertical-align: middle;"></span> Cryptosystems	Sam Coury	Vol 2, Nr 3 (Sep 73)	24
<u>T</u> T/A--Math Symposium Reviewed	David J. Tiren	Vol 1, Nr 5 (Dec 72)	36
Teacher Very Funny	Rich Atkinson	Vol 2, Nr 3 (Sep 73)	19
Things That Go Clank In the Night	Mike Hricik	Vol 1, Nr 4 (Sep 72)	7
Time to Look at People	Tom Glenn	Vol 2, Nr 4 (Dec 73)	19

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

<u>Title</u>	<u>Author</u>	<u>Issue</u>	<u>Page</u>
	<u>U</u>		
Uncertain Origins	Tom Glenn	Vol 1,Nr 5 (Dec 72)	5
	<u>V</u>		
Vietnamese Communist Tactical COMINT Operations	Tim Murphy	Vol 1,Nr 3 (Jun 72)	32
Viet Nam Odyssey, 1972-1973	Leo Stepp/ Ed O'Connor	Vol 2,Nr 4 (Dec 73)	8
	<u>W</u>		
WADE-GILES System	E. Leigh Sawyer	Vol 1,Nr 5 (Dec 72)	35
What Have They Done to our Linguists?	Jeryl O. Gegan	Vol 2,Nr 3 (Sep 73)	14

\* \* \* \*

### Chinese Made Official Language

Agence France-Presse

HONG KONG, Feb. 13 — The government was urged today to draw up a program to improve the standard of the Chinese spoken by residents and to use simple Chinese in its communications with the public.

Hilton Cheong-Leen spoke in support of the official languages bill, which passed. It makes Chinese an official language alongside English.

Steps should be taken, Cheong-Leen said, to avoid use of esoteric and outmoded terms or too literal a Chinese translation of an English original. He also suggested making Mandarin equal in status with Cantonese.

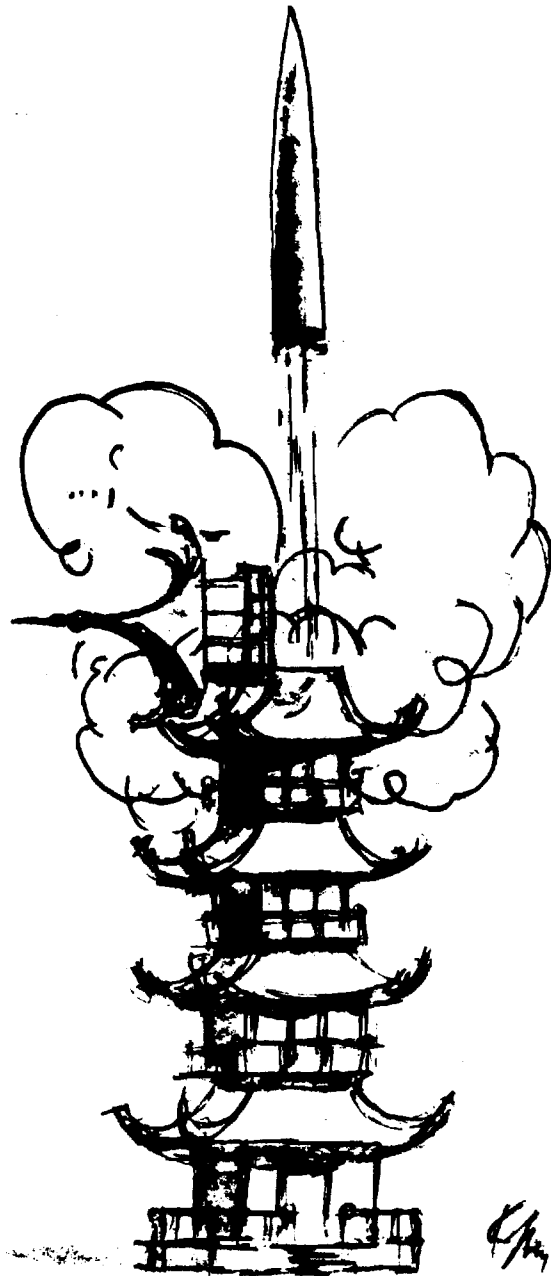
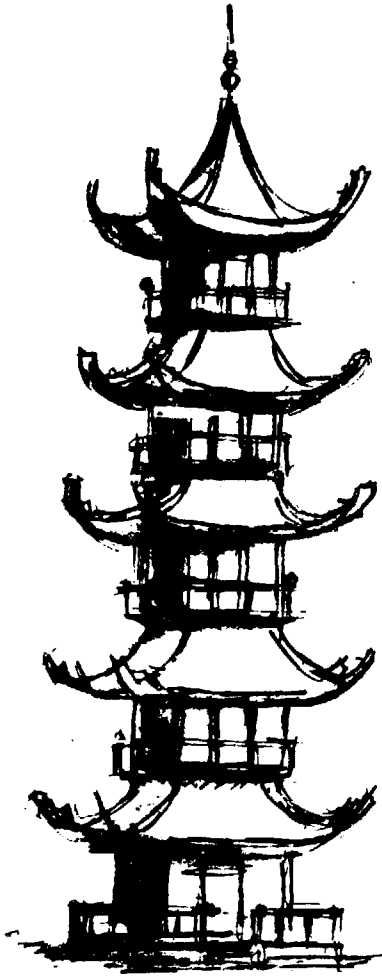
The Washington POST  
February 1974

~~TOP SECRET UMBRA~~

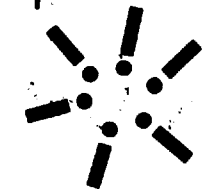


~~TOP SECRET UMBRA~~

A  
CHINESE  
MISSILE



5...  
4...  
3...  
2...



~~TOP SECRET UMBRA~~

~~TOP SECRET~~

JUN 1974?

# National Security Agency

Fort George G. Meade, Maryland



**FINAL EDITION**



# DRAGON SEEDS

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~TOP SECRET UMBRA~~

This is *Dragon Seeds*.

There is fantasy, irony, and the bite of reality in the name. It speaks of the East. And, like the East, it suggests much, says little.

*Dragon Seeds* is both Mother China and her neighbors. *Dragon Seeds* is monumental and minuscule. It is the past and future. It begs for elaboration but gives none. In it are echoed softly slurred Mandarin, brittle Vietnamese, determined Korean. In it is the spectre looming over the Thai, Lao, and Khmer. It is frightening and friendly. It is uncertain.

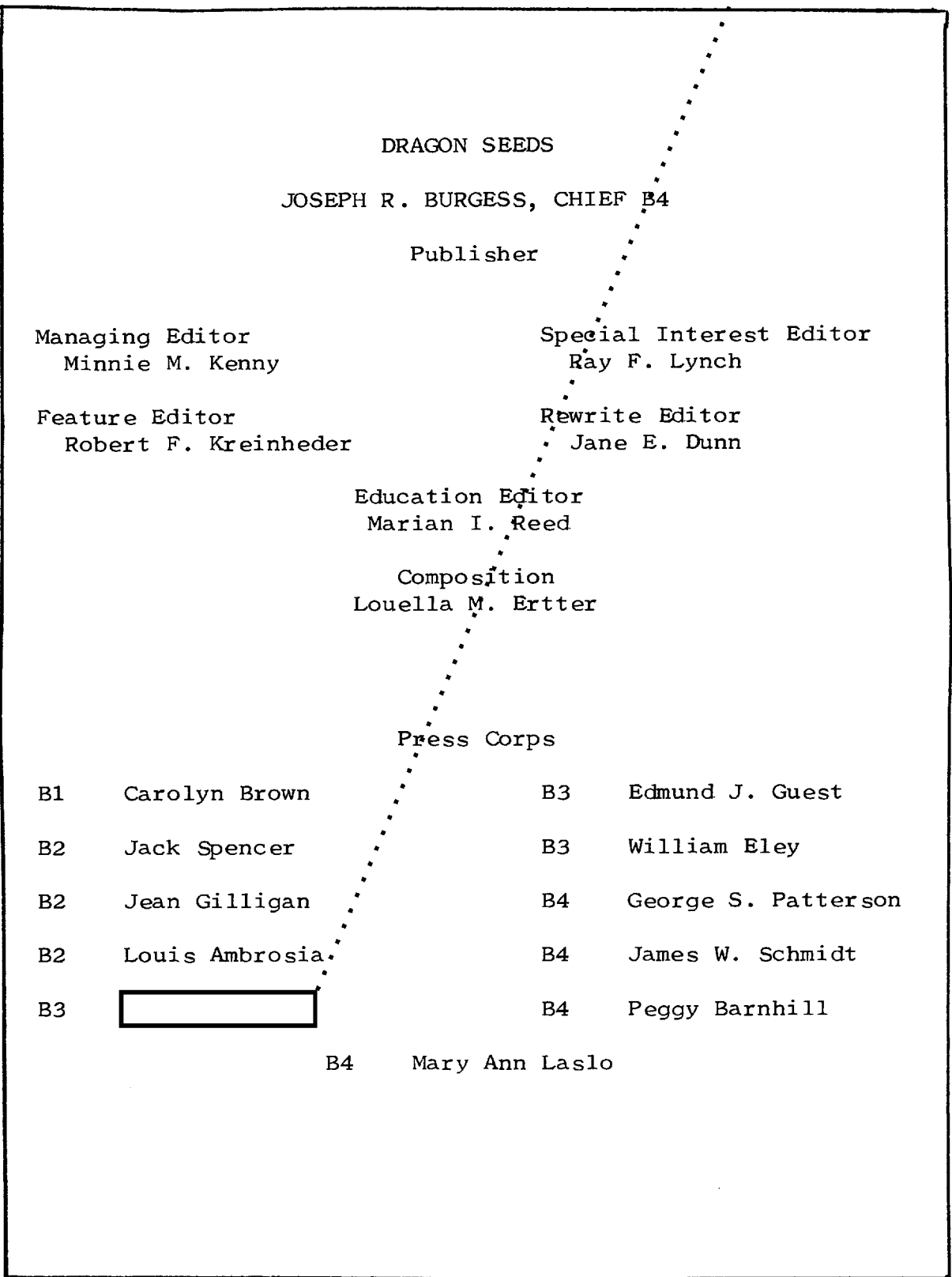
Above all, *Dragon Seeds* is promise. It is fertile with ideas unbounded, to be cultivated with creativity and imagination. It is challenge. It is alive. It will be more than it is.

*Dragon Seeds* is yours. May it grow with you.

The Editors

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~



VOL. 3  
NR II

Final Edition

TABLE OF CONTENTS

Profile of a Rathbone. . . . . Joe Reid 1

The Chinese  . . . . . George Newhouse 7

You Say English Firstly. . . . . John Mollick 11

Laundry Bags, Basketball, Hog Raising  
and  . . . . . Paul Savageaux 13

The Open Door:  
Geopolitical TIC TAC TOE. . . . . Bee Kennard 16

Doing the Twist or Formulas for Finding  
the Expected Number of Canonically  
Transformed Hits. . . . . Mary Ann Laslo 26

The Fable of the Professional Linguist . . . . . Dan Buckley 34

So What Would You Expect?. . . . . Jane E. Dunn 36

Coming Attractions: Chinese Plaintext Statistics 40  
Seedlings 46

Ask the Dragon Lady 50

Contributors 53

~~TOP SECRET UMBRA~~



On Saying Good-bye

For your warm reception of our  
humble offerings....  
Ten Thousand thanks.

For your steady support to  
all our efforts....  
A Million happinesses.

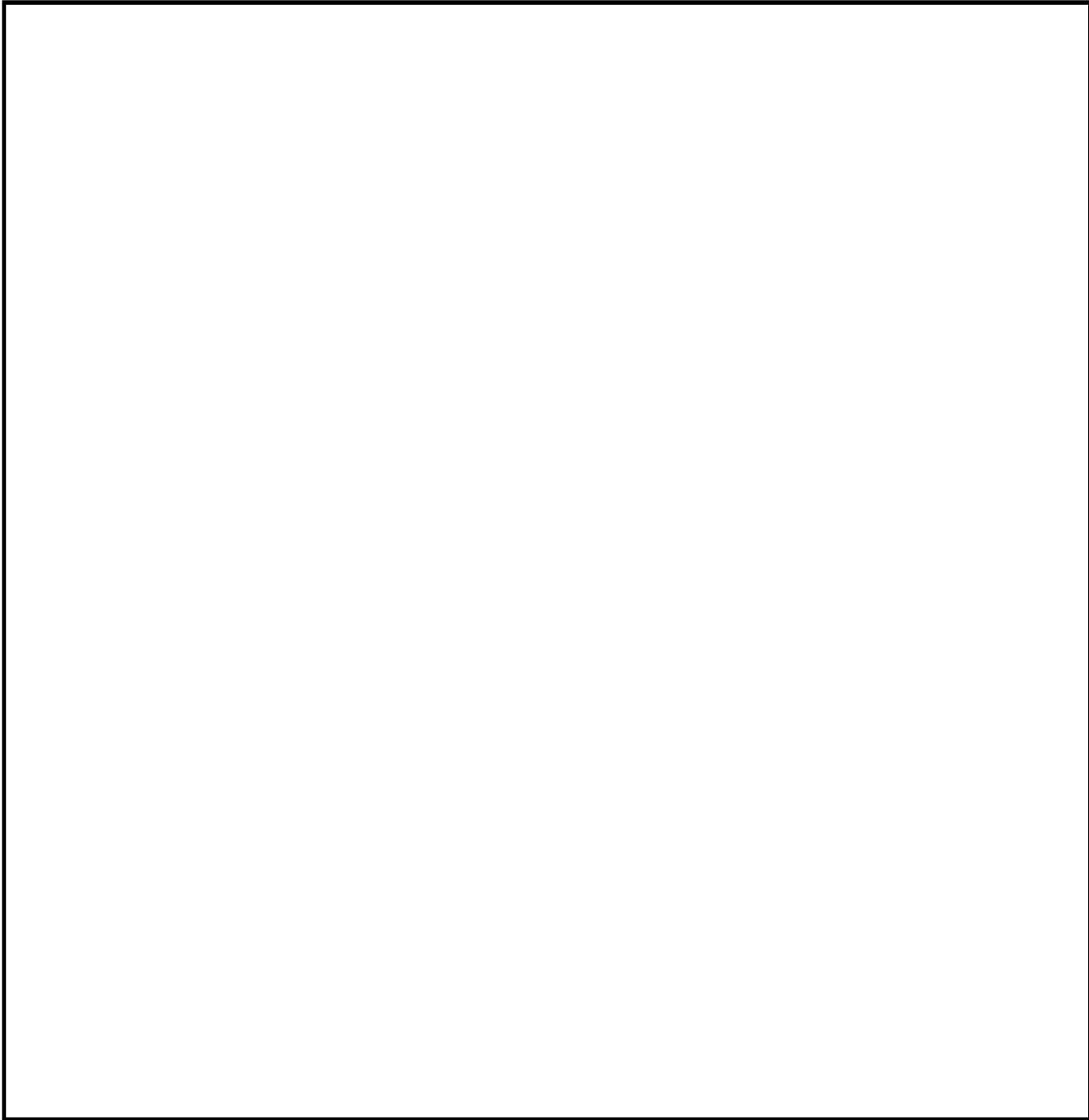
On severing such a close  
liaison.....  
Quintillion sorrows.

*Mink.*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

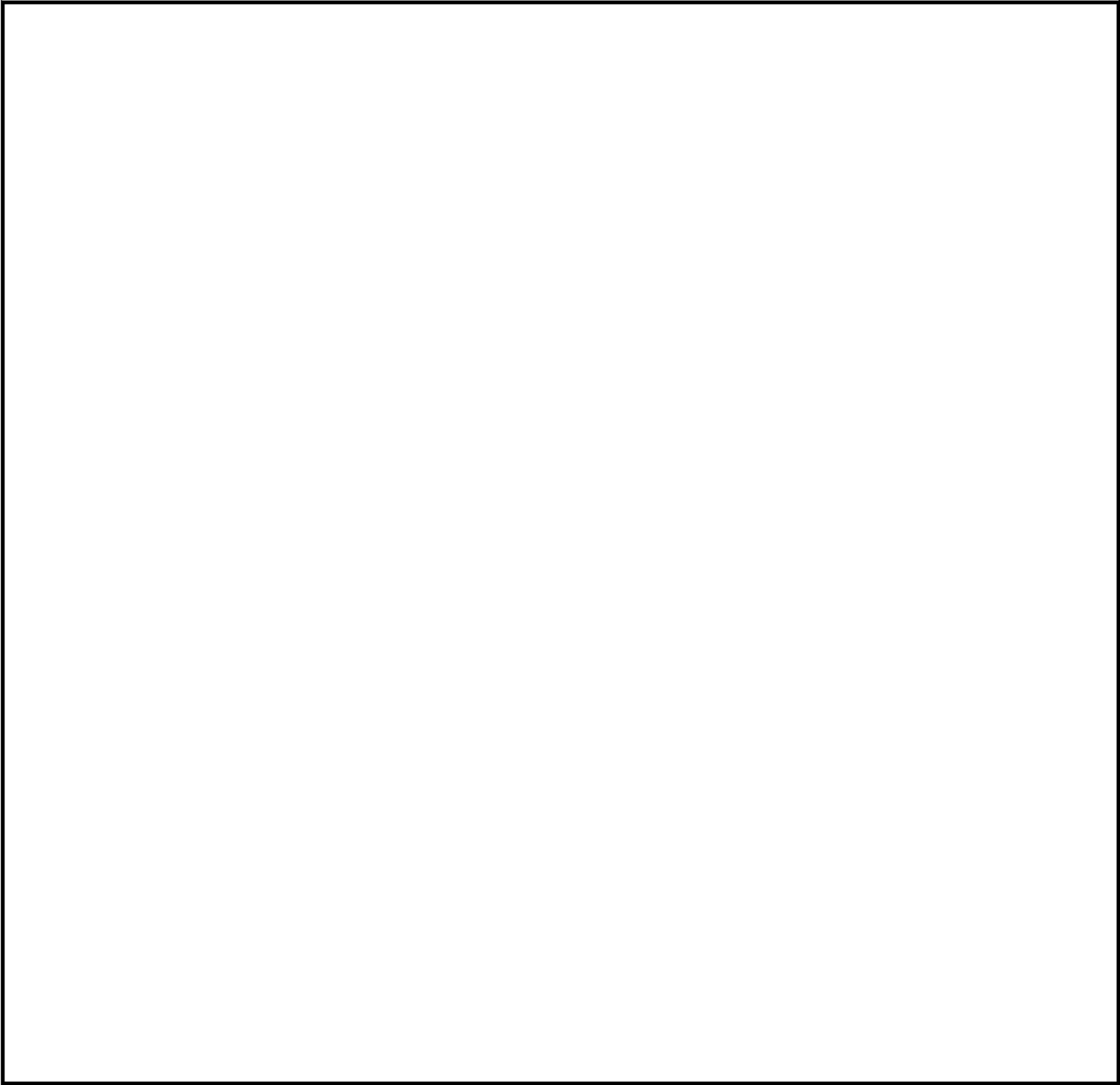
PROFILE OF A RATHBONE  
by Joe Reid, B43



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

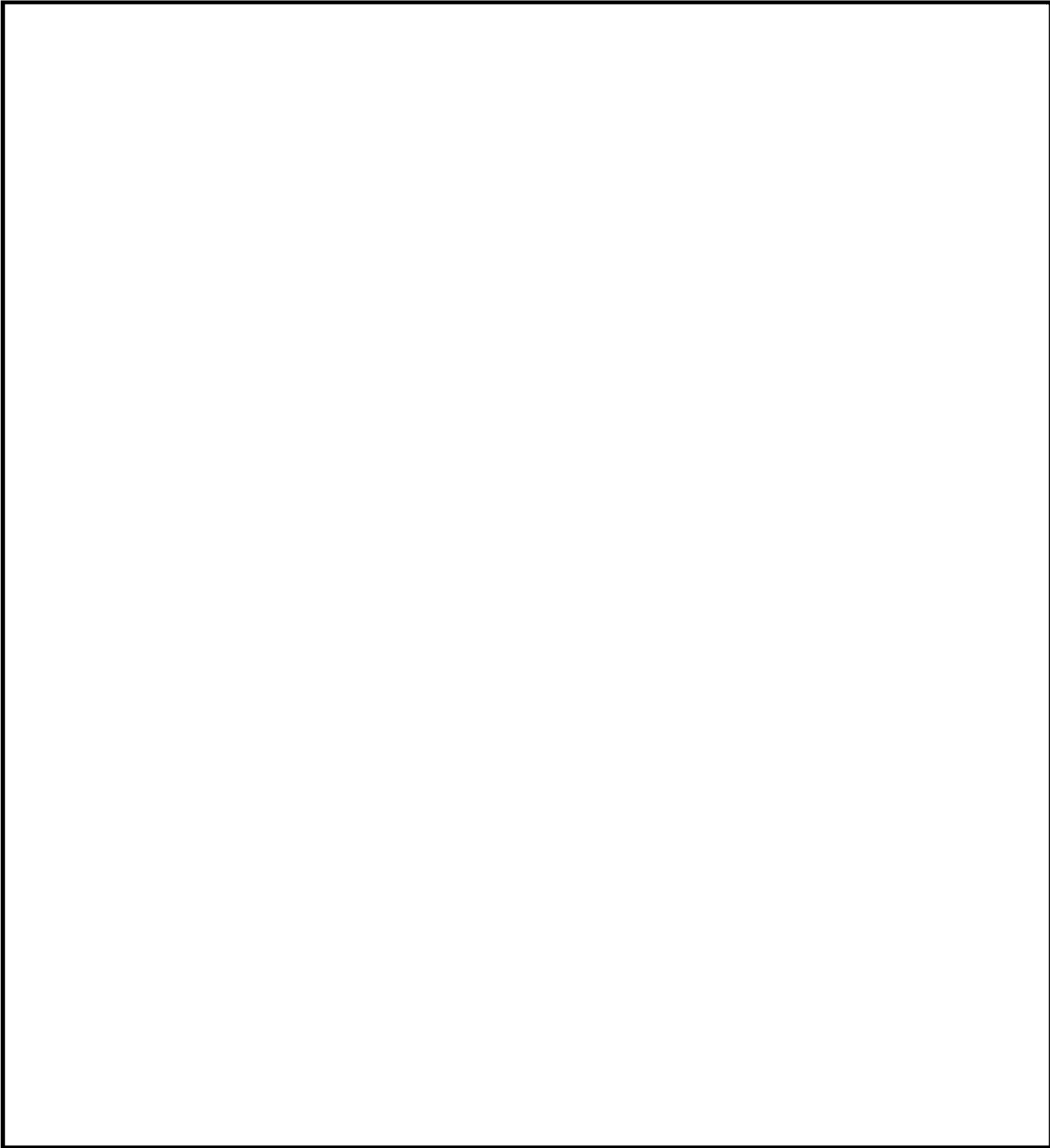


~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

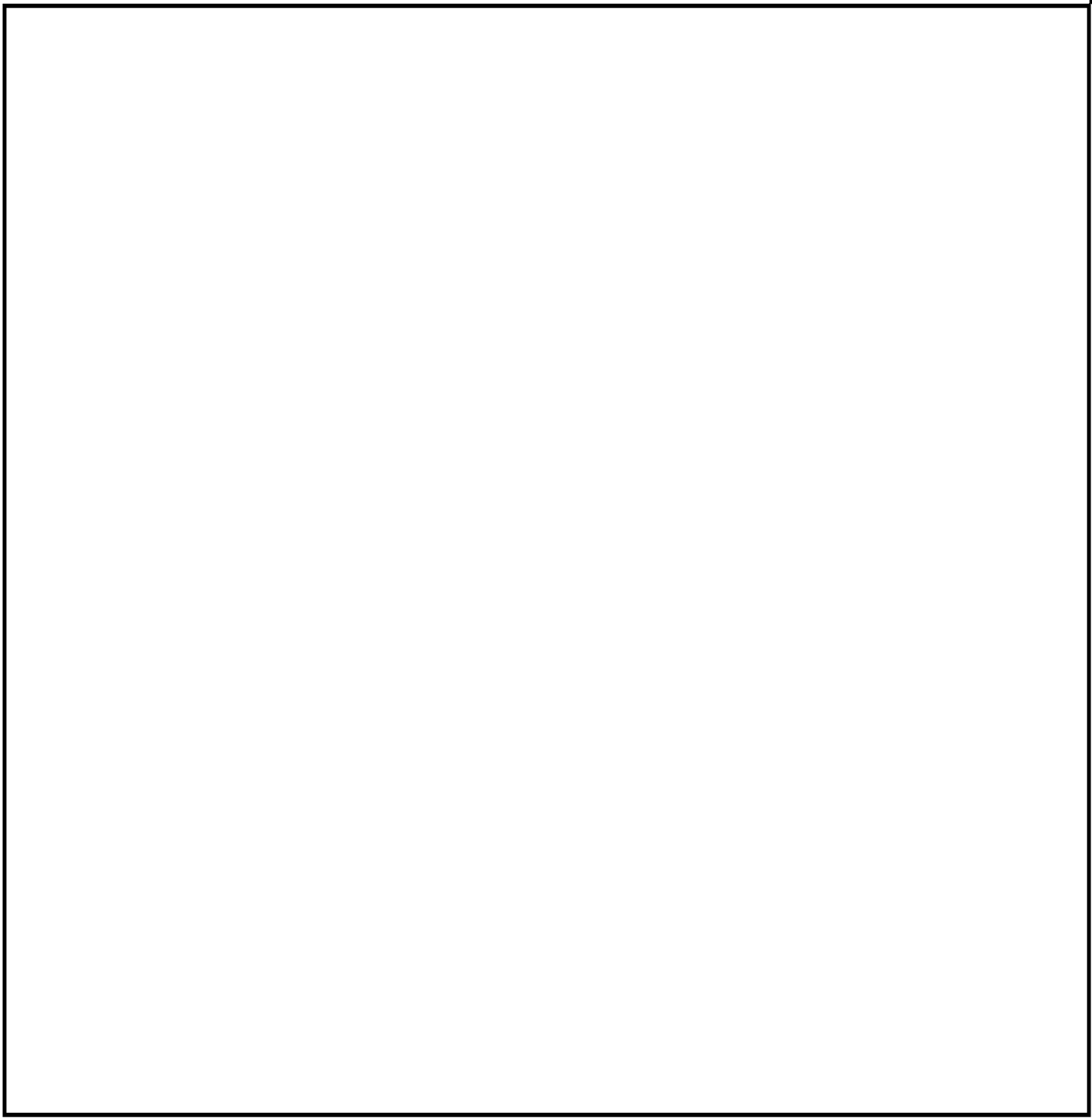
EO 3.3b(3)  
PL 86-36/50 USC 3605



~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

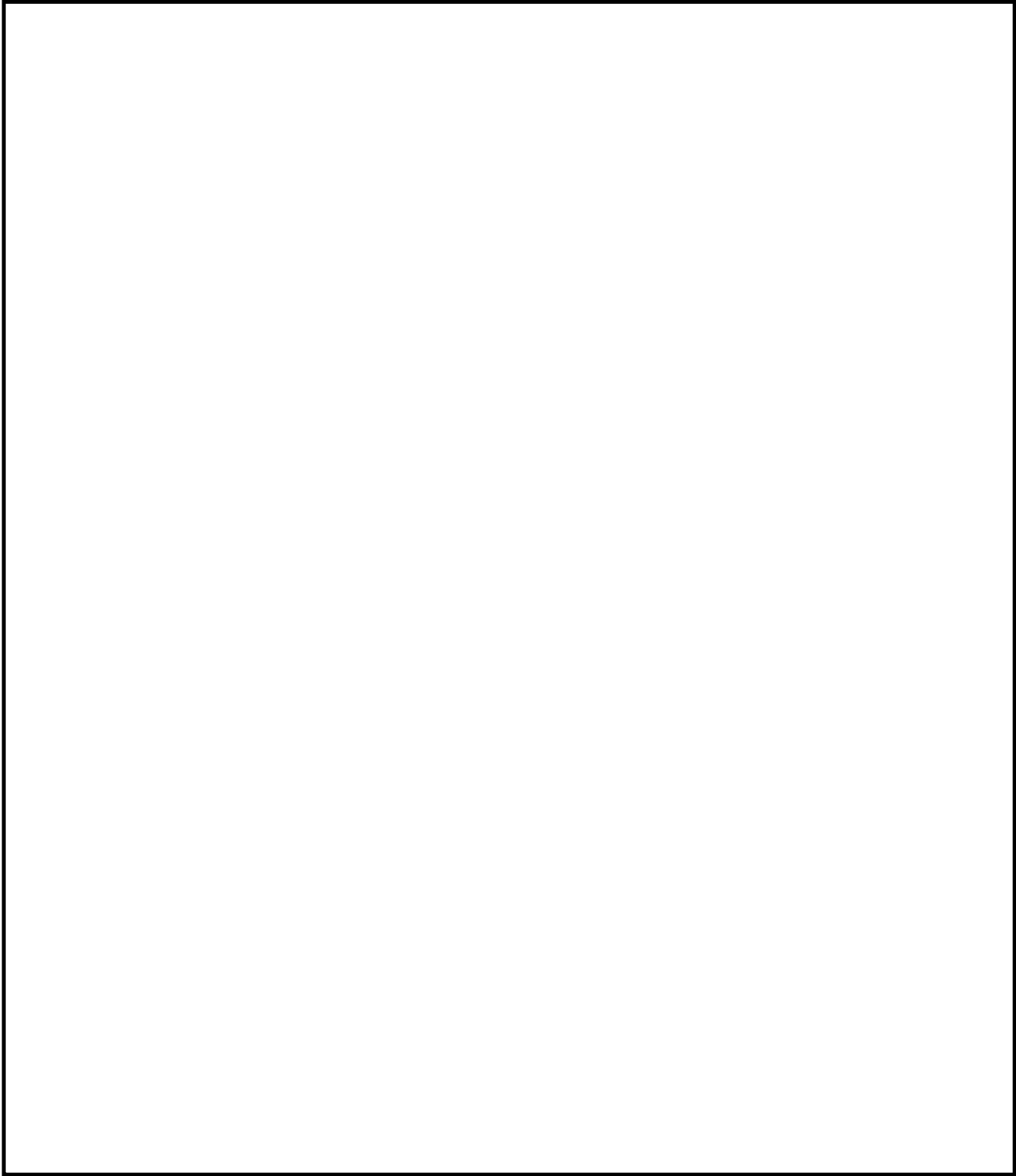
~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



割猪草



下学了，  
割猪草，  
草儿绿，  
味道好；  
猪爱吃，  
又去膘，  
饲养员，  
点头笑：  
说咱红小兵觉悟高。

刘景林诗  
赵广德画

~~TOP SECRET UMBRA~~

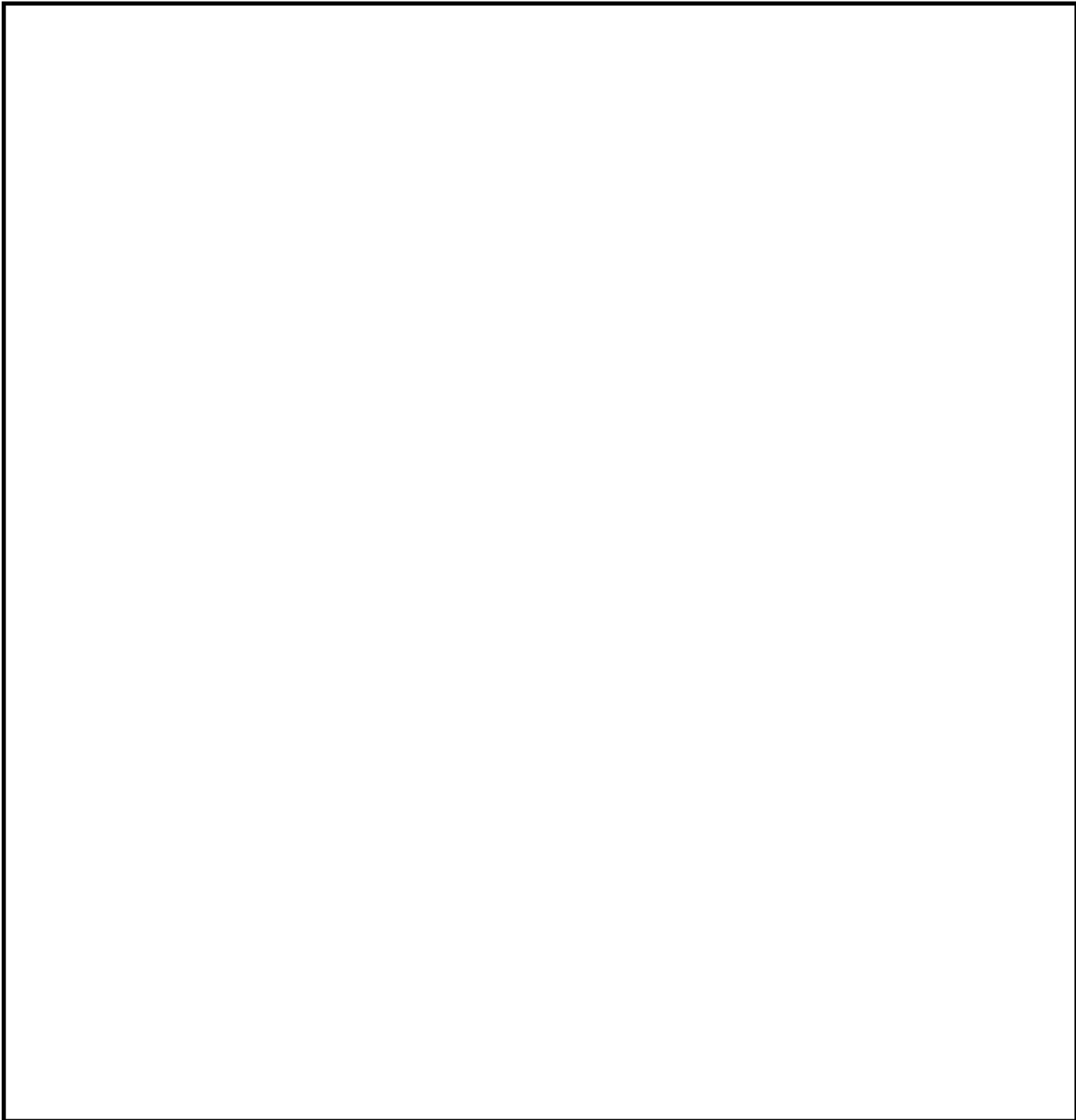
~~TOP SECRET UMBRA~~



THE CHINESE



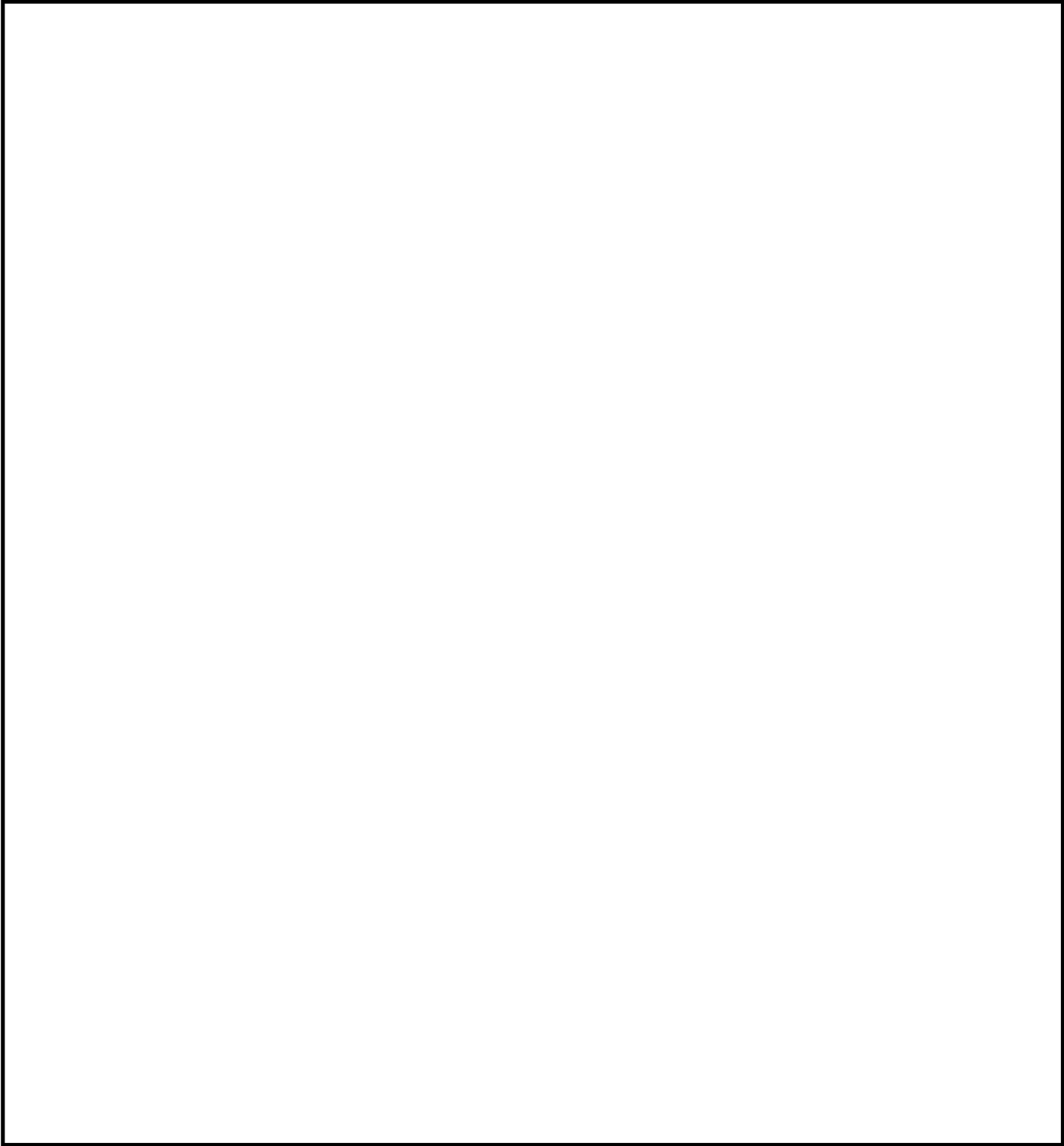
: INFORMATION ALMOST LOST  
by George Newhouse, B21



~~TOP SECRET UMBRA~~

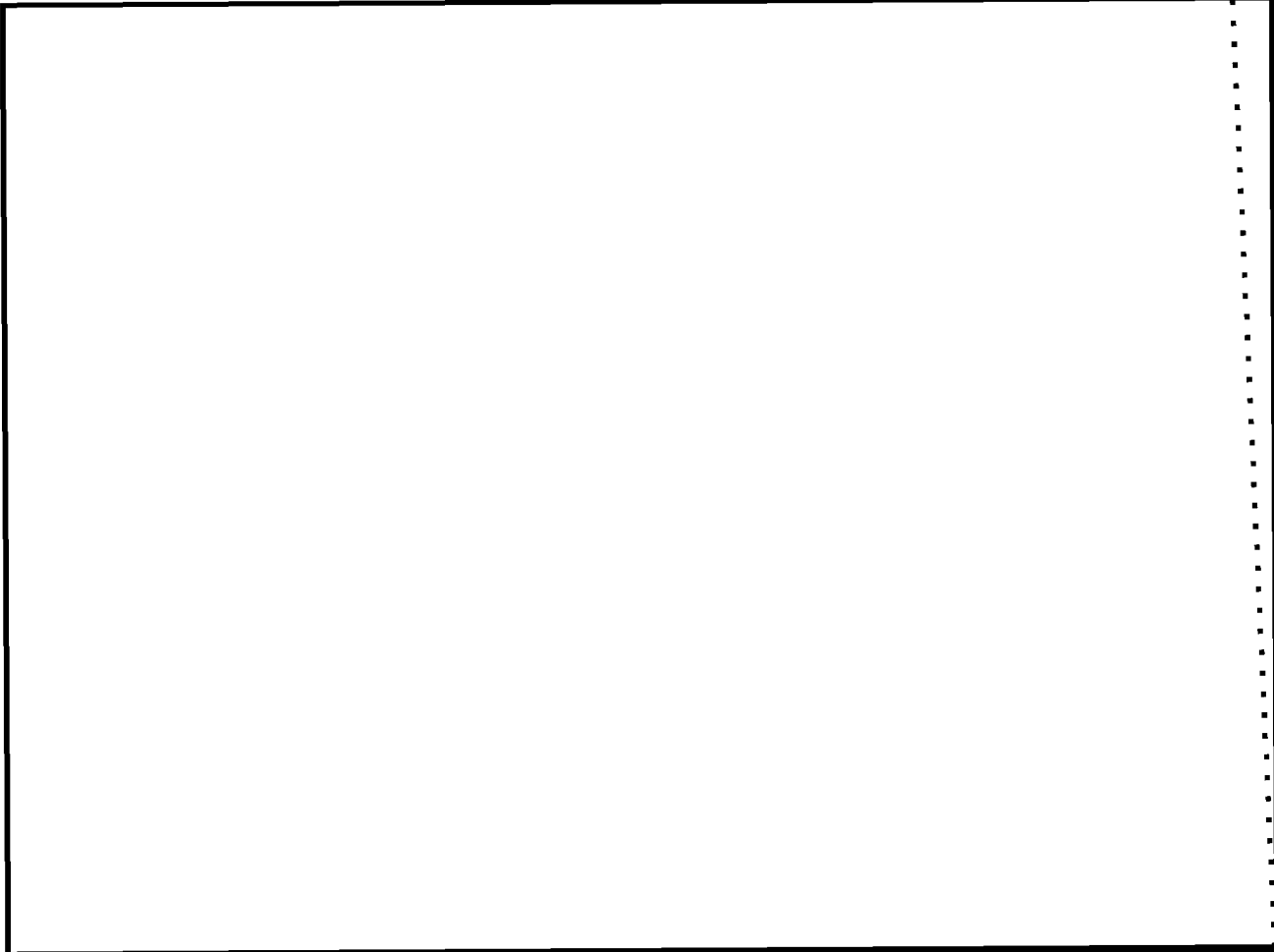
~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



The problems encountered

are

another instance of the age-old human tendency to reject something new, especially when there is no precedent. This tendency frustrates analysts who discover new and unusual information regarding their target country. Because people become so involved with past experiences, new ideas, new solutions and new methods are subject to much suspicion, often resulting in the loss of valuable information to the intelligence community. To avoid these potential losses every analyst and supervisor should make it a personal policy to evaluate new ideas, solutions and methods with an open mind. To paraphrase George Bernard Shaw, we should dream of things that never were and ask, why not?

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



THE PROFESSIONALIZATION OF A SUPER LINGUIST

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

YOUR SAY ENGLISH FIRSTLY! OR DO MY TRANSLATIONS READ  
LIKE THAT?

by John J. Mollick, B25

Have you ever wondered what kind of impression you make on someone whose native tongue is different from your own when you try to demonstrate your "profound" knowledge of his language? Through the years I have gathered a file of erroneous Chinese-to-English translations by non-English translators. The following unexpurgated examples, while humorous, might serve as a reminder that middling knowledge of a foreign language does not a polished translator make.

I have been stolen on my way to the hospital and now in a very embarrass condition.

Younger brother committed suicide by drowning himself to death in the river. That's the fact.

Try as you can to put the personnel on the way to here as earlier as you can do.

He wanted to quit his job for coming back to his native place. "Someone are trying to destroy me," he explained.

I am sick, but I have not been admitted as in-patient to any hospital, so I have to liver and treat my disease in the hotel.

I want to spend three more days to pull out and fill up my teeth. Inform if you approve.

Dear you say English very good too. Your say English too very fine. Your say English firstly.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Tied up in my wife's unchastity, I can't return to unit as scheduled.

The division has provided us with the yarns-spinning workers.

Being treated with torture by your sister-in-law, your younger brother has come to my house and boarding with us a few days.

Not allowed to be discharged from the hospital where he received medical treatment because he was unable to pay the bill, he asked his truck in another city to mail him money.

Sir as I feel urgent please allow me to visit your country.

I'm seized with illness very seriously. If you are concerned, remit money at once; otherwise, leave me alone.

My son, who have been studied for several years at your institute, has failed in the examination because of effortless.

A man from your unit was stolen on leave. He is now at your station for he stole others.

Seminar participants include professors from two universities. Their speak English ability weak.

— • —

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

LAUNDRY BAGS, BASKETBALL, HOG RAISING AND [redacted]

by Paul Savageaux, B21

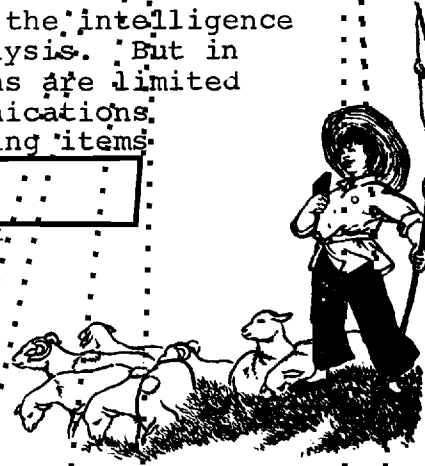
Much has been said and can be said for the intelligence we glean from traffic analysis and cryptanalysis. But in those instances where military communications are limited or where the effective application of communications security exists, other intelligence-producing items must be exploited.

[redacted]

represent.

an exploitable item which provides order-of-battle intelligence. Practically all [redacted] information is obtained from civil communications and collateral sources.

[redacted]



their use as part of the addresses in messages sent in civil communications; designate a unit or organization

[redacted]

The Chinese refer to the

[redacted]

Collateral sources such as newspapers, radio broadcasts, and defector reports many times provide the initial and sometimes the only reference to [redacted]. Such a reference with accompanying information is often the key to unit identification. [redacted] have been reported as appearing on a laundry bag with the [redacted] also printed on it, on the shirts of basketball teams, and in a photograph of a silk banner which contained [redacted] embroidered on it. Each of these were the first indication of the [redacted]

[redacted]

Analysis of plaintext Standard Telegraphic Code (STC) civil communications messages which contain [redacted] yields

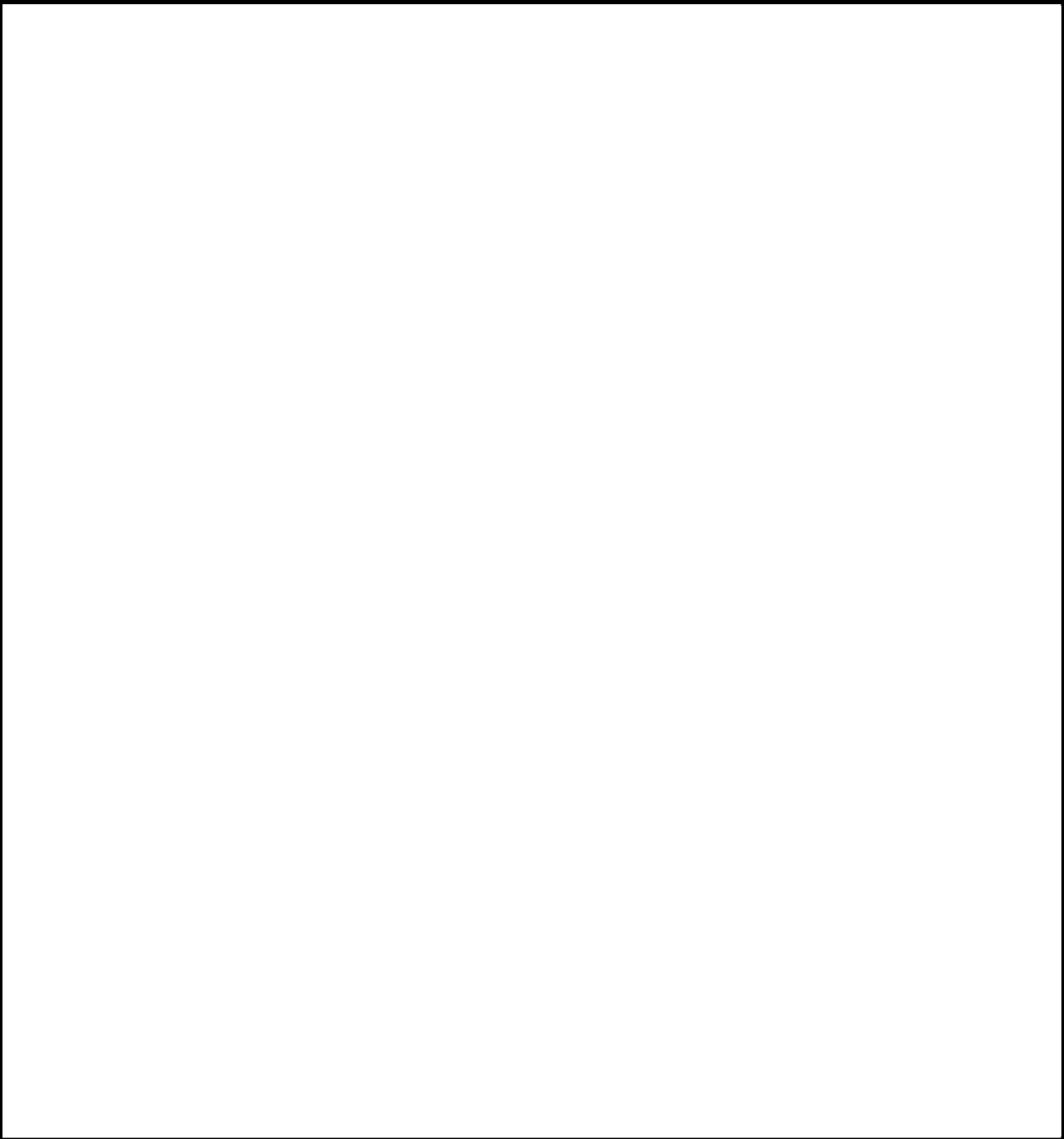
[redacted]

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

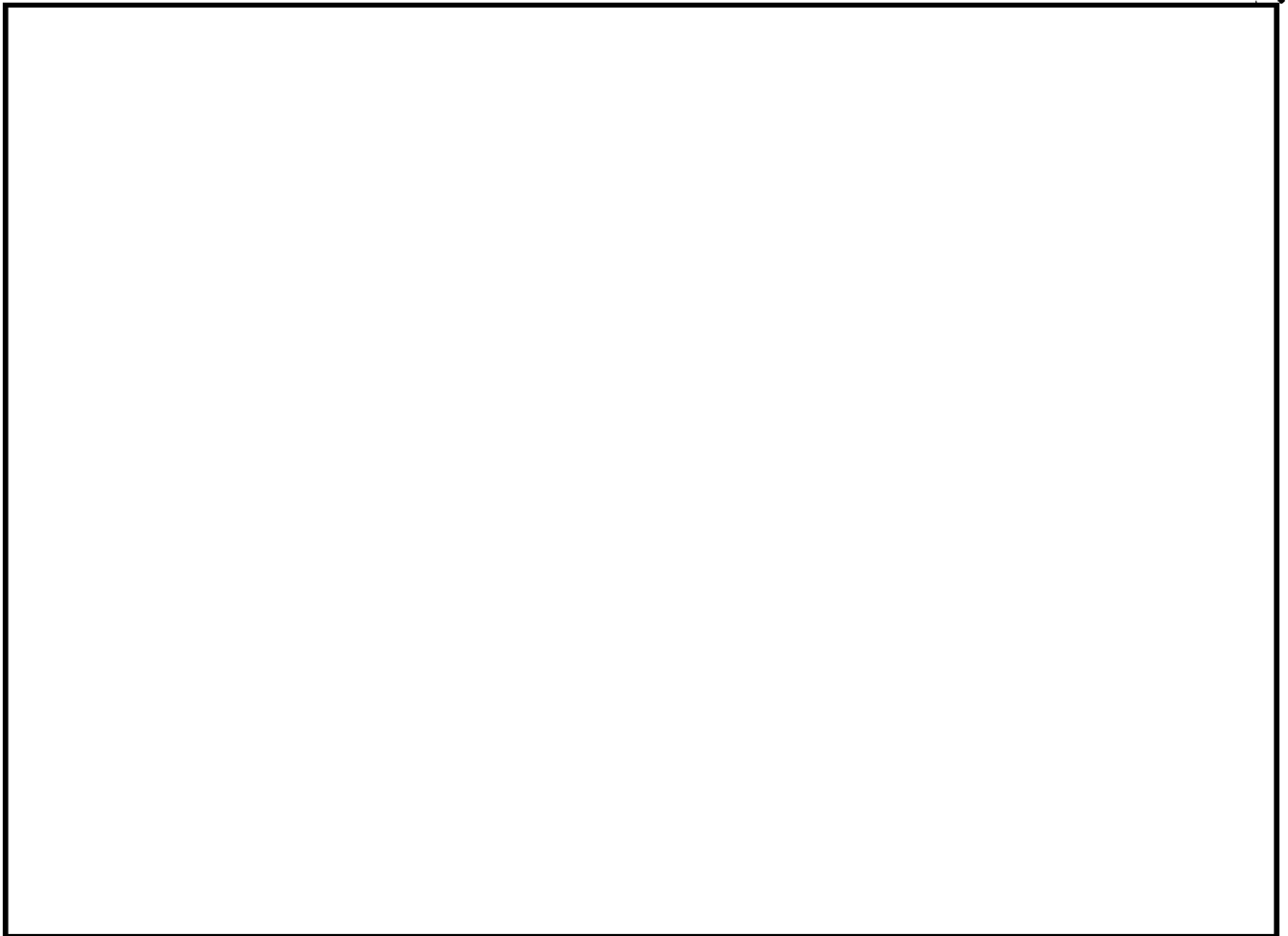
[redacted] provide a valuable means for maintaining continuity on unit locations.



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605



\*\*\*\*

*The camel even when  
mangy, bears the burden  
of many asses.*

*.....Burmese proverb*

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~**THE OPEN DOOR**

*We seek to be companions along the way.  
 The lantern which we carry is not ours.  
 The spirit which we share is contagious thought;  
 The knowledge which we gain, an illuminating torch  
 And all who seek may perceive and learn.*

*-The Concept of Dragon Seeds*

GEOPOLITICAL TIC/TAC/TOE IN THE INDIAN OCEAN

by Bee Kennard, C522

Tic-Tac-Toe and Geopolitics are universal games everybody plays. A world map neatly squared by latitudes and longitudes is the global board which the contestants continually fill with X's and O's. There is the local contest between adjoining countries, the middle game involving the big powers with the locals, and the top level international game among the big powers played for strategic stakes. By combining the two games, the information analyst can see what's happening and where the action is. Since superpower rivalry has just begun in the Indian Ocean, that fluid situation affords an ideal target to demonstrate Geopolitical Tic/Tac/Toe.

Play by Play Description

First, let's start with a calendar of events. The X's represent the political and military offensive moves, and the O's the defensive ones. The plays are then broken down by the game level upon which they are played. Since the undeveloped littoral and hinterland states have neither the desire nor capability of dominating the Indian Ocean, our sample model is limited to India, Australia and those islands and countries linked to the big powers. Due to technical difficulties beyond our control, the following tic/tac/toe game cannot be brought to you in 3D-living color. The split screen and a few winning plays have been selected for this abridged version.

Gamenates on Low and Middle Levels

Gamenote No. 1: This mid-ocean shot shows that the first player has the advantage. The US won on the middle level by taking the center block on the opening play. The rule of thumb

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

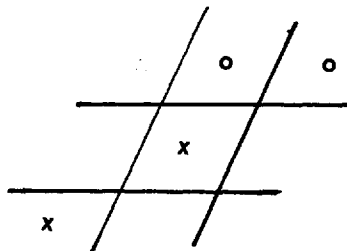
is: first player wins if he takes the center block and the second player doesn't take a corner. If the second player takes a corner, the game ends in a draw.

Gamenote No. 2: The Soviet move into the northwest quadrant of the Indian Ocean exemplifies the draw game. From that area alone the USSR is within striking distance of Poseidon missiles launched from Polaris submarines. If the USSR can secure a base in the northeast quadrant, China comes under a Soviet ICBM threat.

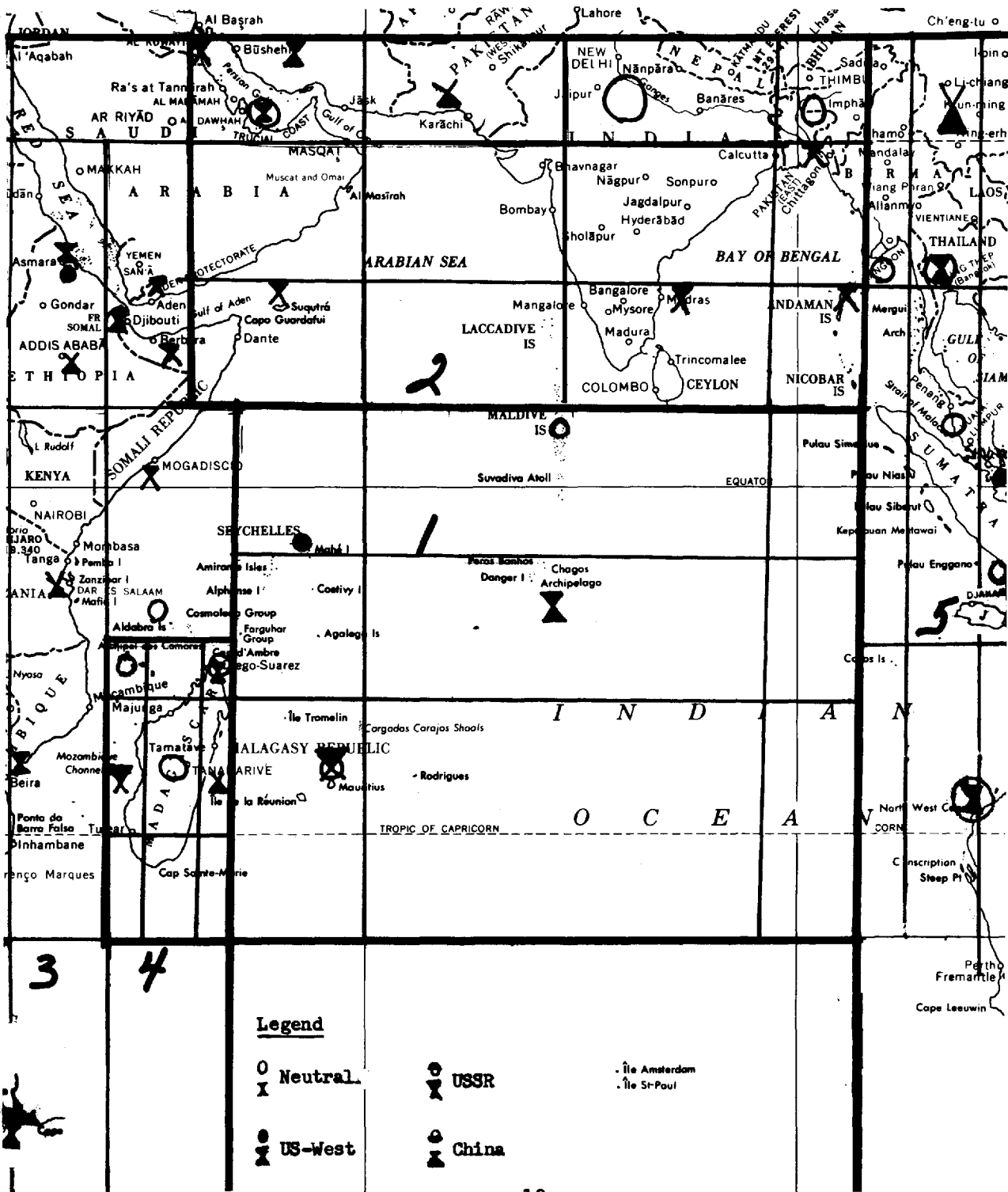
Gamenote No. 3: With acquisition of the Somalia base, the Soviets are in position to score down the East African coast. If South Africa can moor the US to the Cape of Good Hope, then the US can control the southern entrance to the Indian Ocean. In this situation, the rule of thumb is: if both players play the corners, the first player wins who takes the center. Here the 3/T game switches from the offensive to the defensive.

Gamenote No. 4: Madagascar is an historic focal point in naval strategy and it is coming loose. As the defensive center, the third player can block a big power winning play but not successes on the outer fringe. Strategically, the center is the one that counts but half a game is better than none.

Gamenote No. 5: If the third player occupies the center block and plays the inbetween spaces, he can break up any scoring attempts by the big corner powers. The Southeast Asia move to neutralize the Strait of Malacca is essentially a no-win strategy but a tie game is often the best solution regionally and internationally.



# ~~TOP SECRET UMBRA~~



# ~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~Low Toe

- O Maldives becomes independent republic; Britian retains Gan airfield. 26 July 65
- Seychelles and dependencies form new colony named British Indian Ocean Territory. 10 Nov 65
- O Mauritius becomes independent. 12 Mar 68
- X US plans to build radio and aid facility on Diego Garcia. Dec 70
- O Bangladesh achieves independence. Dec 71
- O Australia requests modification of US agreements re communications sites. June 73
- X India and Australia to promote regional cooperation in Indian Ocean. June 73
- O Comorro Islands to become independent. June 73
- O Madagascar withdraws from franc zone; French troops to withdraw by 1 Sept 73. June 73
- O Madagascar bars visit by four US destroyers. 27 Dec 73
- O New Zealand Prine Minister visits India; disapproves large foreign naval presence in 10. 28 Dec 73
- X Portugal offers US a port in East Africa. 26 Jan 74
- X France to strengthen naval presence in 10. 8 Feb 74
- O Australia, New Zealand and Indonesia oppose Anglo-American agreement to expand Diego Garcia 8 Feb 74
- O Magagascar denounces Anglo-American agreement. 8 Feb 74
- X India sends protest notes to US and Britain. 11 Feb 74

~~TOP SECRET UMBRA~~Middle Tac

- X Australia-US agreement to establish naval communications site at North West Cape. May 62- May 63
- X Goodwill visit to India by Commander of Soviet Pacific Fleet Mar 68
- X Mauritius grants landing and docking rights to USSR. July 70
- O India opposed to establishment of naval bases in IO. Nov 70
- X Soviet offer to build submarine base in Andaman Islands. Mar 71
- X India-USSR 20 year treaty of friendship, peace and cooperation. 9 Aug 71
- X Soviet Defense Minister visits Somalia. Feb 72
- X Soviet salvage fleet begins work in port of Chittagong. Apr 72
- X Diego Garcia becomes operational. Mar 73
- X Soviet airfield and longrange communications base set up in Somalia. Apr 73
- O Bahrain orders US Navy to leave dock facilities. 29 Oct 73
- X USSR formally requests standing port facilities in India. 20 Nov 73
- X Mauritius signs agreement with USSR on aircraft landing rights. 23 Nov 73
- X Brezhnev visits India. Soviet arms aid pledged. 26-30 Nov 73
- X USSR seeks renewal of salvage contract with Bangladesh. 19 Dec 73
- X China-Ethiopia establish air link; China offers to provide arms. Dec 73
- O US-Australia agree to operate North West Cape jointly. 10 Jan 74

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

- X China-Madagascar sign economic, technical and trade agreement. 18 Jan 74
- X Soviet Foreign Affairs bureau chief visits Tanarive. 1 Feb 74
- X China-Pakistan agree to build SAMs. 21 Jan 74
- Kagnew communications base to close 30 June 74. Feb 74
- Australia rejects Soviet request to build joint satellite tracking station. 10 Apr 74
- X South African Commander in Chief visits US privately. 7 May 74



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~Top Tic

- Soviet UNGA proposal Indian Ocean be declared nuclear free zone. 7 Dec 64
- ✕ Soviet warships visit Indian Ocean ports. Mar-Nov 68
- ✕ Soviet naval visits increase. 1969-70
- Britain announces withdrawal East of Suez by end 71. Jan 69
- Lusaka resolution of nonaligned countries to keep IO Zone of Peace. Sept 70
- ✕ Commonwealth Head of Government conference in Singapore to consider Soviet naval threat in IO. Jan 71
- US contemplating denuclearization proposal re IO to USSR. Apr 71
- Brezhnev calls for curtailment of cruises by navies in distant waters. June 71
- Southeast Asia declares region Zone of Peace, Freedom and Neutrality. 27 Nov 71
- ✕ US strike carrier Enterprise enters Bay of Bengal during Indo-Pakistani war. US intends to send naval forces into IO from time to time. 13 Dec 71
- UNGA resolution declaring IO Zone of Peace. Resolution sponsored by Ceylon calls for complete demilitarization. China endorses resolution; US and USSR abstain. 16 Dec 71
- US-USSR discuss how to avoid naval arms race in IO. Tacit agreement to limit bases. 1971-72
- ✕ NATO announces Britain and Netherlands to conduct patrols in IO. Dec 72
- ✕ US sends naval task force into Indian Ocean 29 Oct 73
- ✕ US Navy to visit IO on a more frequent and regular basis. 30 Nov 73

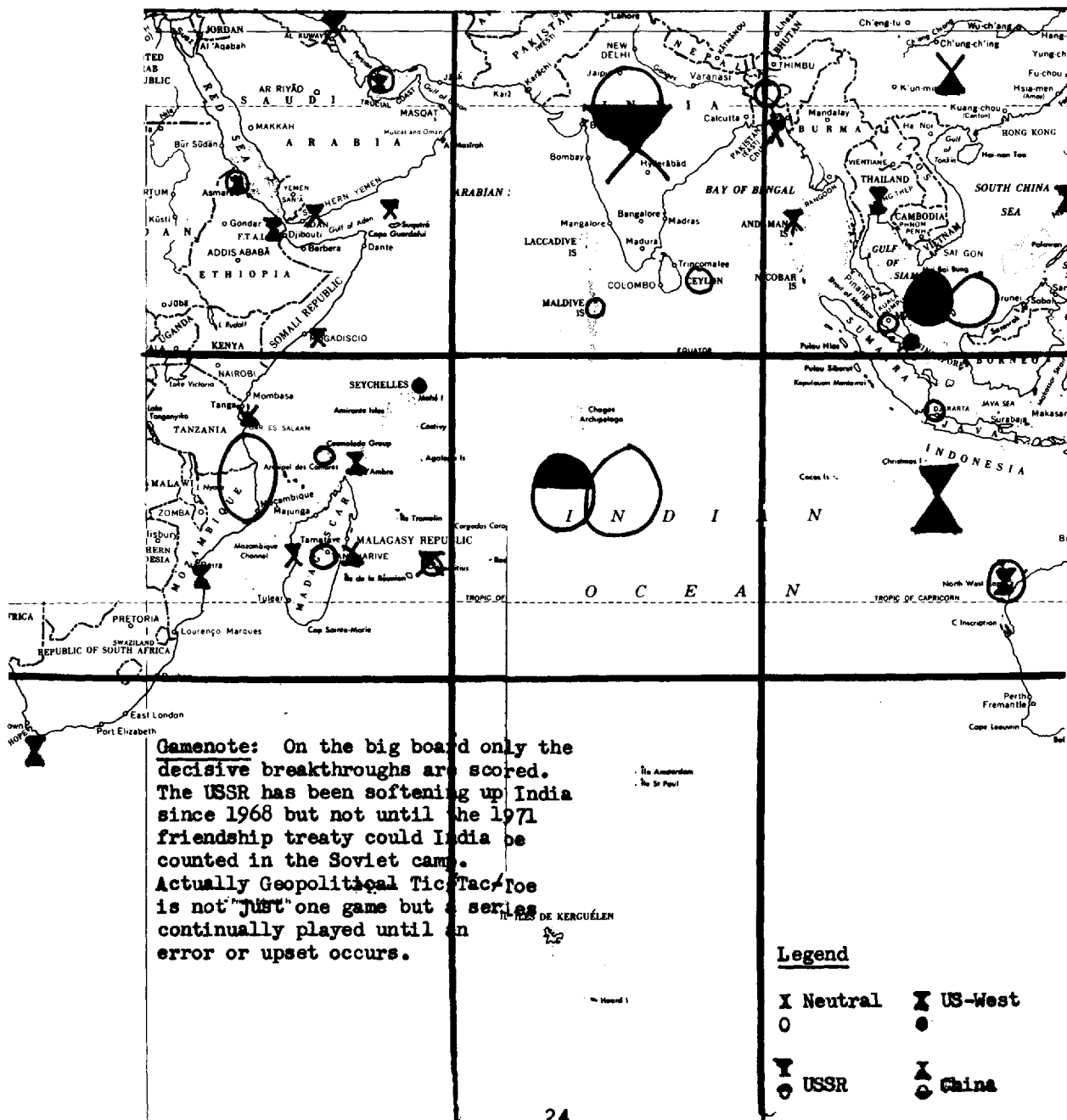
~~TOP SECRET UMBRA~~



# ~~TOP SECRET UMBRA~~

## 3/T Formation

Next, let's take Top Tic, Middle Tac and Low Toe and superimpose them on a map of the Indian Ocean.

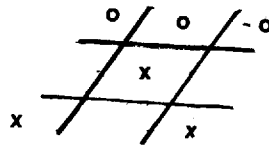


~~TOP SECRET UMBRA~~Monday Morning

Now the analyst can actually see how the geopolitical game shapes up in the Indian Ocean. On Middle Tac the US has scored a diagonal tic/tac/toe with communications sites from Ethiopia to Diego Garcia to Australia. Likewise the USSR got in on the ground floor at the US and together with the neutralists was winning the international political game. However, the US decision to expand Diego Garcia into a support base has dramatically changed the strategic outlook in the Indian Ocean. The deployment of a US naval task force to the Persian Gulf during the Middle East confrontation forcibly reminded the Soviets of the SLBM threat from the Indian Ocean and served notice of US intentions to protect the oil life-lines to Japan and NATO.

South Africa is attempting to cash in on its strategic gateway astride the oil lanes from the Indian Ocean. A western military alliance would enhance its reputation whereas Southeast Asia is trying to get out from under and into the neutralist camp.

Neutralist efforts to preserve the neutral character of the Indian Ocean come too little and too late. Big power rivalry to fill the vacuum left by British withdrawal East of Suez is well under way. In a word, the Indian Ocean is up for super-power grabs. However, rules and predictions seldom allow for human error so upsets are frequent in the balance of power contest. If at first you don't succeed in geopolitics, try patience and persistence.



x o o o x

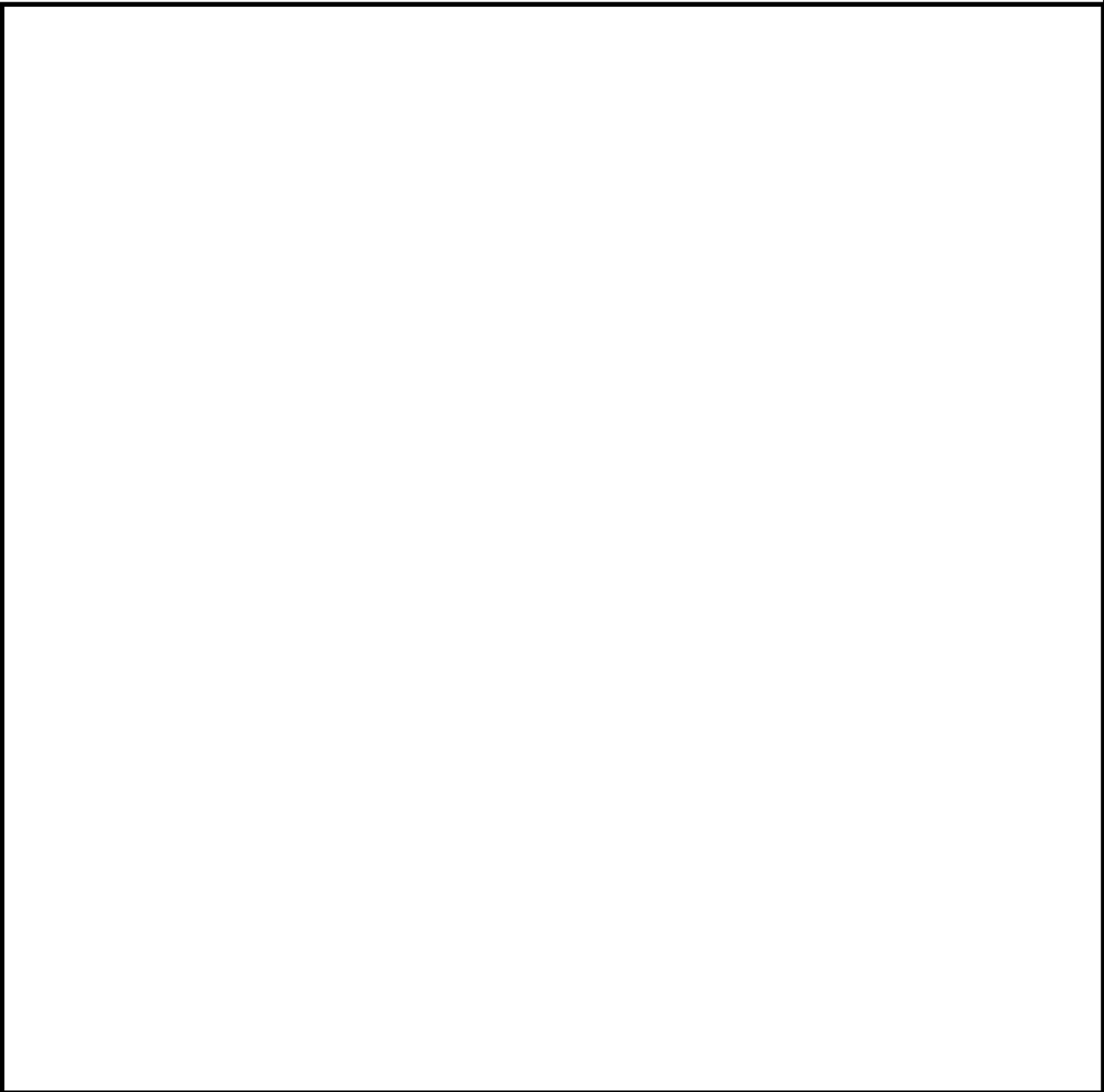
~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

EO 3.3b(3)  
PL 86-36/50 USC 3605

DOING THE TWIST OR FORMULAS FOR FINDING THE EXPECTED NUMBER  
OF CANONICALLY TRANSFORMED HITS (TRANSPOSED GROUPS) WITHIN  
A GIVEN SAMPLE

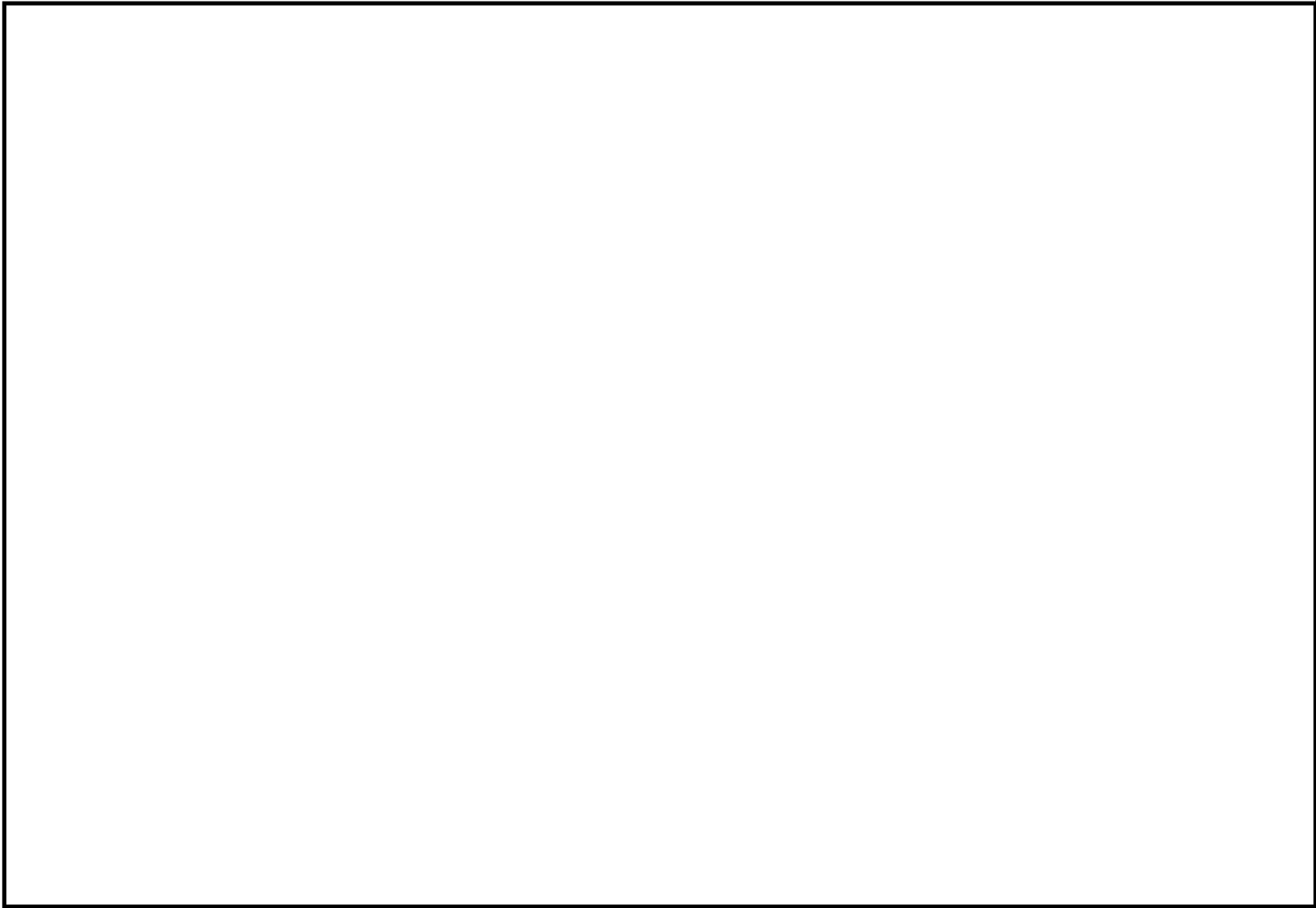
by Mary Ann Laslo, B43



~~TOP SECRET UMBRA~~



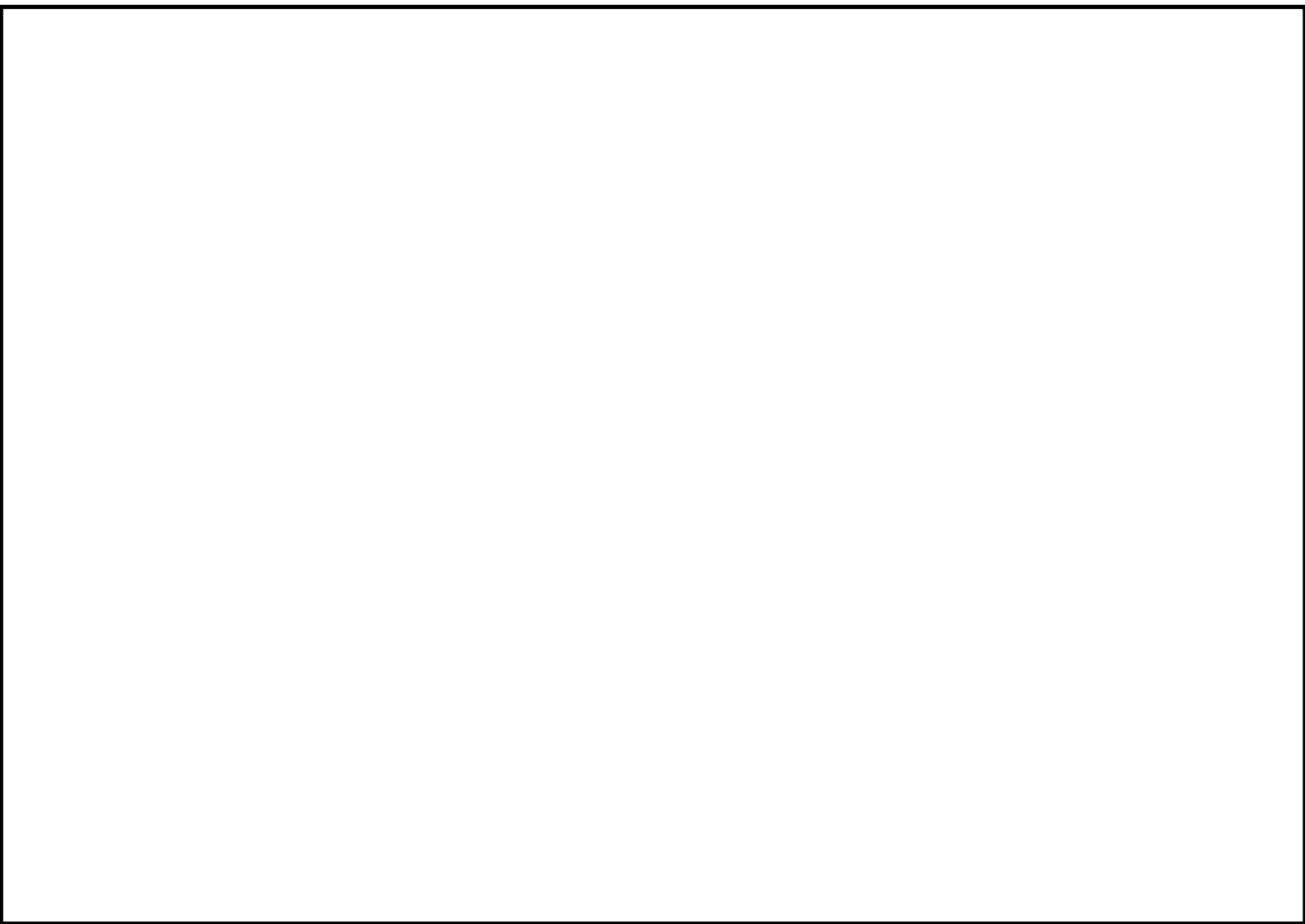
EO 3.3b(3)  
PL 86-36/50 USC 3605



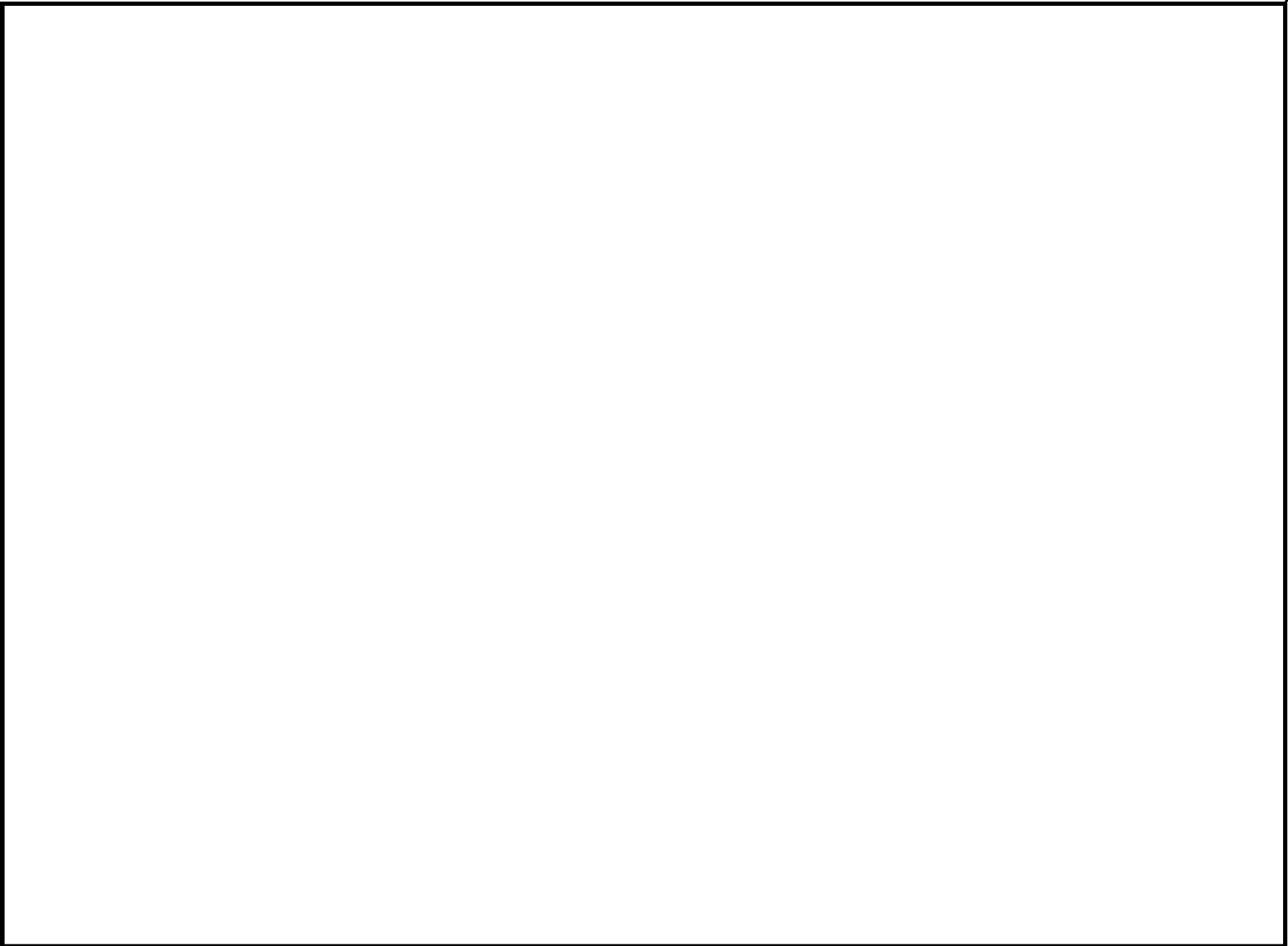
~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

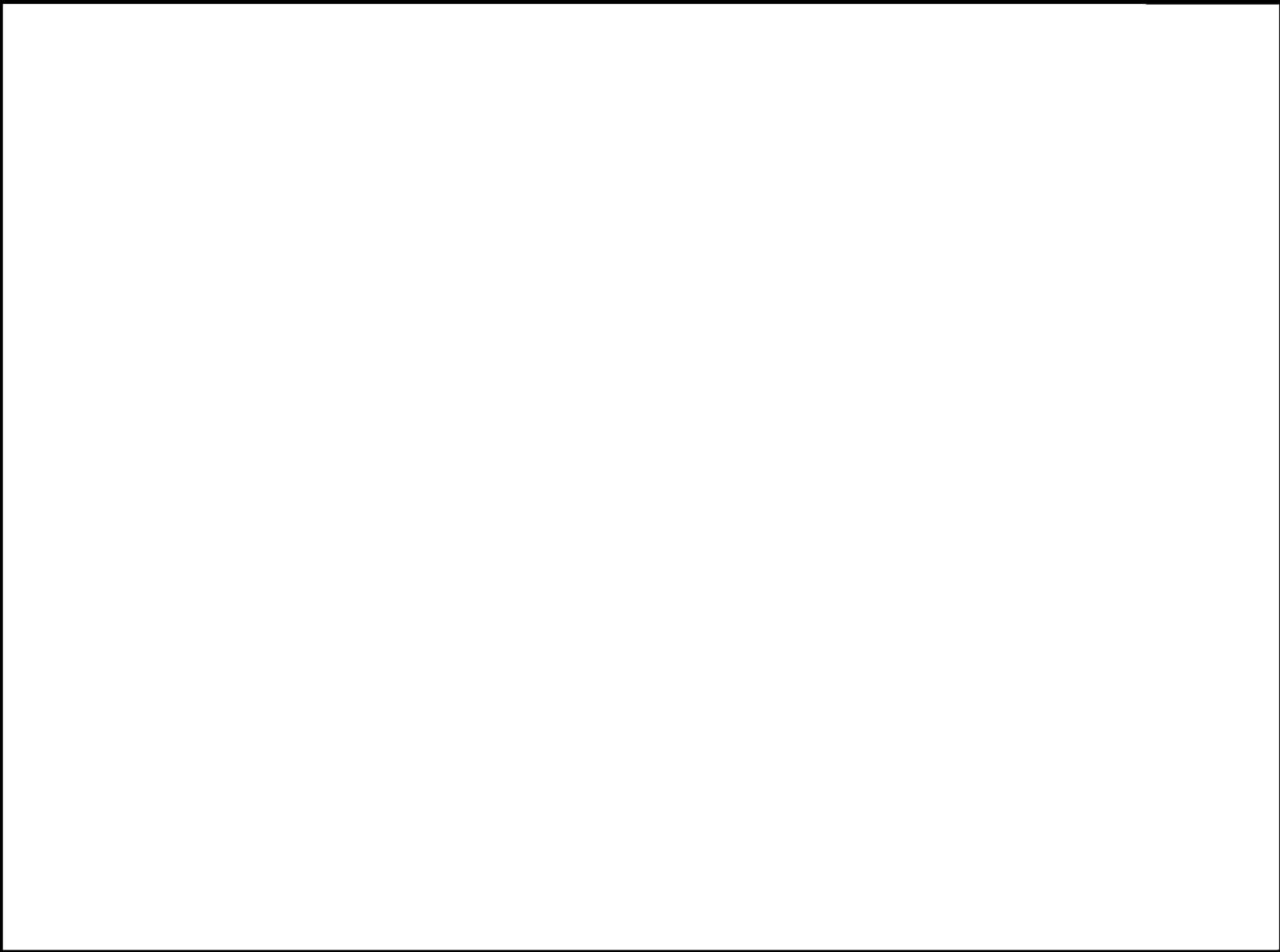


~~TOP SECRET UMBRA~~



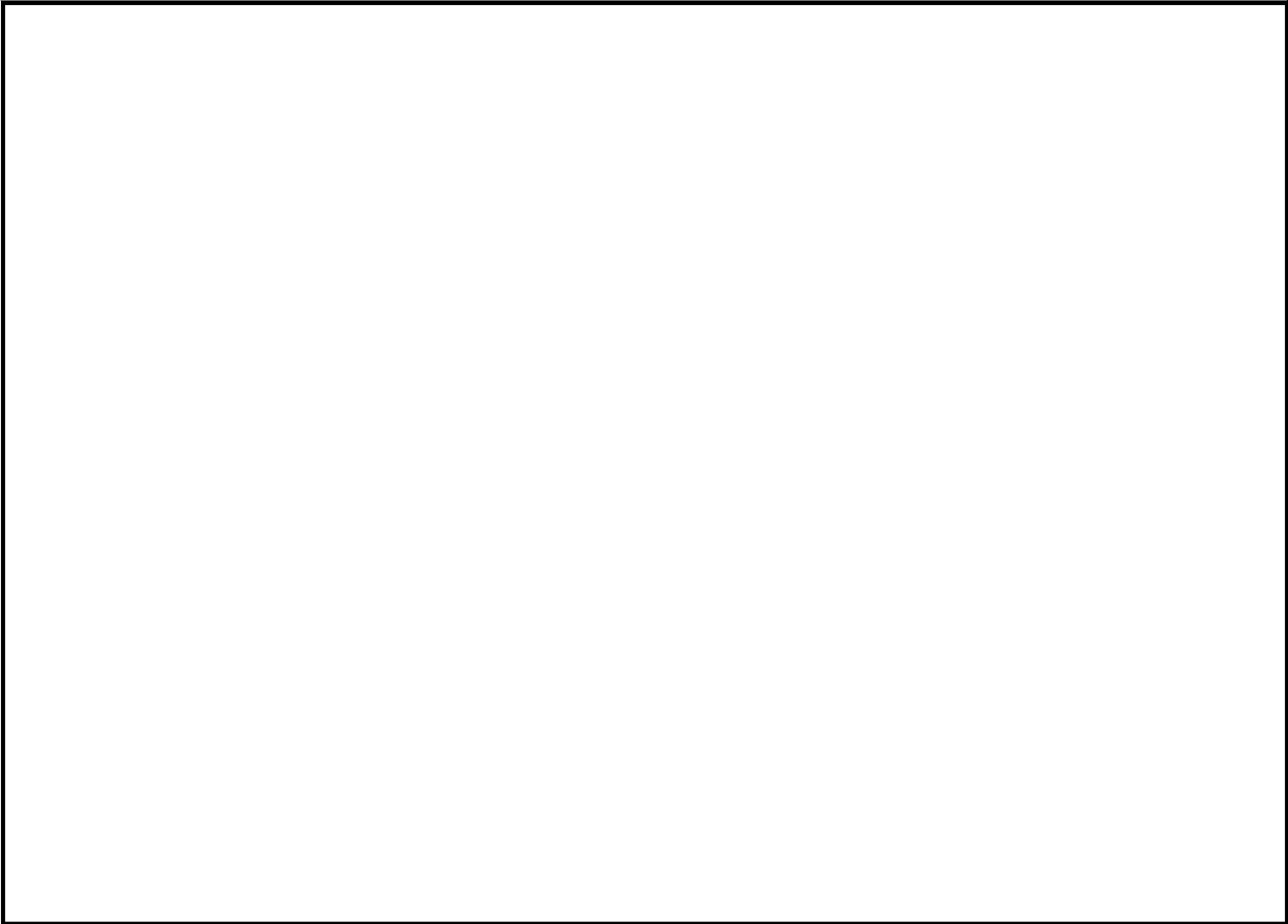
~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

東洋의 山

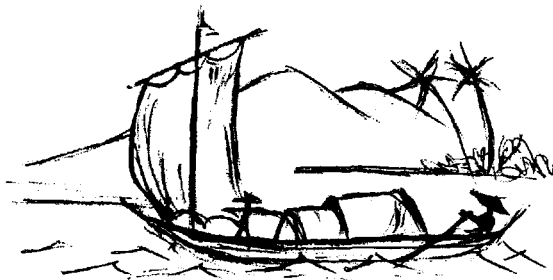
이 한 직

비 썩 마른 어깨가  
 抗議 하는 양 날카로운 것은  
 솟 았 았 고는 못 참는  
 애 달픈 天堯 을 타고난 까닭 일꺼  
 다  
 激 한 噴火 의 記 憶 을 지 냈 다  
 그 때 는 어린 대로 심히 慙 해  
 볼 수 도 있었 기 때문 이 다.  
 植 物 들 은 해 마 다 헛 되 히  
 뿌 리 를 뺐 으 나  
 끝 내 森 林 은 이루 지 못 하 였 다  
 지 나 치 게 悽 愴 함 을 겪 고  
 나 면  
 오 히 려 이 런 게 도 마 음 코 오  
 해 지 는 것 알 까

THE HILL OF THE ORIENT

YI HAN-JIK

THAT MY BONY SHOULDERS ARE SHARP  
 AS IF IN PROTEST  
 PERHAPS IS FROM THAT IMPATIENT  
 TEMPER OF MINE  
 WHICH SEES AND MUST ACCUSE.  
 I CARRY MEMORIES OF VOLCANIC  
 VIOLENCE;  
 FOR THEN I WAS FREE TO BE FURIOUS.  
 MY PLANTS HAD ROOTS, IN VAIN,  
 EVERY YEAR  
 AND NEVER GREW TO BE A FOREST.  
 IS IT BECAUSE I HAVE WALKED  
 THROUGH TOO MANY CRUELITIES  
 THAT I AM IN SUCH QUIETUDE?  
 I HAVE NOW NOTHING TO INSIST UPON.



~~TOP SECRET UMBRA~~

이제는 固執 하여야 할 아무  
主張도 없다

지금 山기슭에 "부주카" 砲가  
震動하고

共產主義者들이 낯설은  
外國말로 喊聲을  
올린다

구리고實로 믿을수 없을 만큼  
손쉽게

쓰러져 죽은 善意의 사람들  
아 그러나 그 무엇이 나의 이고요  
함을

깨칠 수 있으리요

눈을 꼭 감은 채

나의 表情은 그대로 얼어붙었나  
보다

微笑마저 잊어버린

나는 東洋의 山이다

AT THE MOMENT

THE HILL-SIDES SHAKE FROM THE  
BAZOOKAS;

THE COMMUNISTS RAISE SHOUTING  
IN ALIEN TONGUES;

AND THOSE GOOD-WILLED PEOPLE  
HAVE FALLEN SO EASILY

THAT I CAN HARDLY BELIEVE IT.  
BUT, NOTHING CAN DISTURB ME OR  
MY QUIET NOW.

WITH TIGHT CLOSED EYES,

THE ICE OF MY EXPRESSION FREEZES  
HARD.

I, WHO EVEN HAVE FORGOTTEN HOW  
TO SMILE,

AM THE HILL OF THE ORIENT.

TRANSLATED BY KIM JONG-GIL

道

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

THE FABLE OF THE PROFESSIONAL LINGUIST

By Dan Buckley B32

Once upon a time in the sleepy country of NSALAND, near Washington, D.C., a strange animal was born. Now, in many countries this event would have been newsworthy, perhaps even reportable in a WAR or other weekly, but this mother had given birth to such strange animals in the past that little attention was paid and the new arrival, called professional linguist, was more or less ignored and allowed to grow or not grow as he chose.

Being an aggressive animal, professional linguist chose to grow and discovered much to his liking that he flourished on various colored pieces of paper called traffic. Also much to his liking, he found that supervisors truly appreciated the way he devoured the traffic feed, routed it through his internal circuitry and regurgitated it in some form comprehensible to those animals different from him, who almost always were larger than he. But he did grow. From seven to nine he went, then to eleven, and lo, even to twelve. He truly realized his nature by this time and in that realization he also came to know that the animals larger than he did not fully understand him. Oddly, he thought, they often kept on growing while he had stopped. As the years passed and he grew no more, he wondered about this mysterious affliction that had befallen him. Examined by all sorts of other professionals, there appeared to be nothing lacking in his external forces: performance appraisals, awards, certification, etc. But nothing would make him grow. He ate more traffic, wrote more translations, fissioned another certification, and was adored by all. Nothing! Then one day, one of the larger animals asked him: "Why do you not become a different kind of animal. Everyone knows that linguists are bright and skilled, especially professional linguists, but they are always so small. If you want to become a larger animal, you must certainly start by becoming a different animal."

Professional linguist was crushed. It had simply never occurred to him that the mysterious affliction haunting him was the nature of the beast itself. He could not believe it and he went in search of professional linguists who had grown larger than 12. After many months of searching, he found one who had grown to fifteen and was considered to be a veritable wizard. The wizard listened to the dilemma of the smaller professional linguist and sympathized with him. In the end,

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

he admitted that very few professional linguists had grown greater than twelve while eating traffic. More important, the wizard explained the process of metamorphosis to professional linguist. It was simple: he had only to stop eating traffic, to leave the eating of traffic to smaller linguists and he would grow. His diet would consist largely of timecards, performance appraisals, activity reports, and hinkel ham sandwiches. Except for the ham sandwiches, he found the fare not nearly so tasty as the multicolored paper traffic feed, but it was indeed more nourishing. Very soon he grew to thirteen and his hopes for further growth were bright.

Much to his delight, he found that he was not alone as a metamorphosized linguist, as he thought he surely would be. NSALAND was literally crawling with them and along with them, he gorged himself with hinkle ham and said words like "management" and "interface", which he did not truly understand. But no matter, because he no longer understood the language with which he was born either and it seemed entirely appropriate.

The moral of this fable is: Wet birds don't fly at night (which makes about as much sense).

\*\*\*\*

*"Chairman," said Mrs. Mao,  
 "You sigh and you pucker your brow,  
 Your fingers are weaving like knots --  
 You're having, perhaps, second thoughts?"*

...Johns Hopkins Magazine  
 June 1974

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

SO WHAT WOULD YOU EXPECT?

by Jane E. Dunn, B4 TDT

You are a manager among whose newly acquired responsibilities is the production of intelligence information from encrypted messages of a SIGINT target. Your personal background is firmly in T/A and reporting, and you have always felt that CA was an esoteric art that an outsider could not really appreciate. Now you must sit in judgment of people and operations in that "foreign" field. What should you expect of a crypt effort? More pertinently, what should you expect of the cryppies involved in it? If your deputy is an experienced, professional cryptanalyst, you have some breathing space, but the responsibility is still yours. Here are some thoughts from one professional cryptanalyst and erstwhile manager which may help.

The good crypt effort, whether manned by one or one hundred people, is marked by a "professional" outlook. Its operations are oderly, comprehensive, and documented. Its members characteristically use the scientific method of systematic pursuit of knowledge yet are flexible enough to allow for and to profit from the intuitive leaps that sometimes bring solutions. The effort progresses as far along the path of diagnosis, solution, exploitation as the resistance of the systems and the human and machine resources to attack them will permit. Individually and collectively, the crypt group keeps itself informed about advances in cryptanalysis against other targets through reading technical publications, participating in professional assemblies and conferences, and obtaining advanced training to increase and sharpen skills both in crypt and in related SIGINT disciplines. The group and its members keep in close touch with the non-crypt aspects of its own its own target problem, making sure that the exchange of information is two-way.

An indispensable part of the professional and scientific effort--in crypt as in any other technical discipline--is documentation. The manager should expect that procedures and results will be put on the record. Formal or informal reports published in the appropriate technical series are minimal requirements. Publication in the NSA Technical Journal will give wider dissemination to good ideas and may bring the author and his problem the bonus of professional recognition outside his immediate area. Encourage technical reporting.

With the "professional outlook" established as a necessary base, what about the work the cryppies do? How does a non-cryptanalyst judge cryptanalysis? Perhaps the manager cannot

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

expect to penetrate the interdisciplinary wall, but some aspects of the actual work can be assessed by an outsider. Good marks go to goal-oriented work--organizational goals, that is--rather than to work which only satisfies the personal likes of the individuals doing it. If the work can meet both objectives, so much the better. You should look for attributes such as initiative, imagination, innovation, and enthusiasm tempered by practical good judgment about potential results. There should be an evident willingness to learn about and to use modern methods and tools such as computers and to maintain and improve individual technical skills.

Technical reports and records, published and unpublished, formal or informal, can let you see what is going on and can help you to evaluate the crypt effort, its directions, and prospects as well as its people. Read them.

The cryptie knows he has reached a solution when the system "reads." The manager has no such definite measure in evaluating a crypt effort. Perhaps these few ideas can provide a sort of check list or starting point to help him arrive at a reliable judgment about this part of his responsibilities.



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Here are some thoughts on the kinds of documentation a cryptanalyst should keep. There will be some omissions depending on whether the analyst is working on an exploitation or a research problem, on a bookbreaking or a diagnosis problem.

A cryptanalyst is a record keeper and classifier, and he owes it to his employer to keep those records outside his own head and in such form, content, and volume as will be accessible and useful to contemporary and future analysts and managers.

1. System descriptions (encrypt versions), samples of traffic, decrypts, product.
2. Key recoveries, code recoveries--up to date.
3. Oddities and cryptocharacteristics by system, target, correspondent.
4. Plaintext logs and indexes.
5. Traffic counts and logs.
6. Descriptions of work done--approach, procedures (including computer program names, descriptions, and output), results.
7. CIP (or whatever it is now) documents; lists of isologs and possible depths.
8. Pertinent TA and collateral information; captured cryptomaterials' structure and use.
9. Pertinent information about predecessor and contemporary systems of the same or related targets.
10. Translated decrypts of particular intelligence interest.
11. Proper names encountered; target's names for institutions, practices, organizations, and materials.
12. Crib lists.
13. Notes to the next comer--"try these first".

Not to forget when wrapping up a problem to prepare a vital records package (on microfilm probably) including a technical report.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The official technical records such as system descriptions, traffic counts, TEXTA information, should be in the official vehicles for such records--for crypt, the Crypt Status Report--and in such published documents as crypt identification guides, etc. But they should also be part of the "package" the working cryptie keeps for his own problem. CI information should be published in the appropriate product series. It is all part and parcel of the analyst's not hugging knowledge to his breast as though it might diminish his stature if someone else knew about his problem, progress, or techniques. He needs to get it on the record so others can make use of it.

\*\*\*\*

SAYINGS OF THE SAGES :

The real fault is to have faults and not try to amend them.

Pale ink is better than the most retentive memory.

To go beyond is as bad as to fall short.

Knowledge is boundless but the capacity of one man is limited.

An inch of time is worth more than a foot of jade.

Settle one difficulty, and you keep a hundred others away.

過猶不及

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

COMING ATTRACTIONS:

Statistics on Chinese Plain Text

BACKGROUND

Over one million characters of Chinese plain text represented as CTC (Chinese Telegraphic Code) groups and recorded on magnetic tape were given to NSA [redacted]. The CTC groups were translated to STC (Standard Telegraphic Code) and recoded from the Honeywell Tip Top to the Burroughs 6700, the 6700 providing quick turn-around on debug programs.

The study of this file was undertaken for two main reasons:

- a. To support cryptanalysis [redacted]
- b. To provide Chinese linguistic information for language training at NSA, the CETA (Chinese-English Translation Assistance) Groups, and [redacted]

A committee was formed by Ken Cohen, then in B45, to design the programs for the statistical analysis of this huge data bank. The committee members were:

- B03 Linguist, Norman Wild
- P15 Crypto-mathematician, Catherine Krafft
- B43 Cryptanalyst/mathematician, Mary Ann Laslo (x3755s for general information).
- B42 Programmer, Alton Gowen
- B42 Programmer, Michael Cavanaugh
- B42 Programmer, Richard Neal (x4823s for program information)

In addition, Dave Claybrook, B4TDLA, provided the Chinese graphic characters for the runs; and Ed Stoops, B44, and Elsie Flemming (now retired), B441 provided general English meanings for the STC groups and helped to proofread the output listings.

It was decided to publish the output statistics in four parts:

- Part I Statistics on STC Data-Digital (Tetranomic) Form
- Part II [redacted]
- Part III Statistics on STC Data-Literal (trigraphic) Form.
- Part IV [redacted]

Only parts of Part I (those of linguistic interest) will be distributed outside NSA.

**TOP SECRET UMBRA**

**TOP SECRET UMBRA**STATISTICAL STUDY, Part I

The [ ] STC File Statistical Study, Part I, is almost completed, and should be available sometime in June 1974. Part I, "Statistics on Digital (Tetranomic) STC" will be published as a B441 Working Aid, and will contain the following information.

1. MONOMES- each of the four positions-in-group and all four positions combined:

- a. frequency distribution
- b. percentage
- c. repeat rate
- d. gamma I.C.
- e. total sample size

2. DINOMES

- a. dinomic frequency distribution
- b. percentages
- c. repeat rate
- d. chi square statistic
- e. gamma I.C.
- f. total sample sizes for the dinomes:

A, B)		A, Al)	
A, C)		B, Al)	
A, D)	within group	C, Al)	Across group studies
B, C)	studies	D, Al)	
B, D)			
C, D)			

A, B, C, and D are the four positions of an STC group, and Al, Bl, Cl, and Dl are the four positions of the group immediately following that group.

3. TRINOMES

- a. inverse frequency listing of the 100 highest frequency trinomes
- b. repeat rates
- c. chi-squared statistics
- d. total sample sizes

The above are given for each of the following trinomes:

A,B,C)		C,D,Al )	between group
A,B,D)	within	D,Al,Bl)	studies
A,C,D)	group studies		
B,C,D)			

# TOP SECRET UMBRA

## 4. TETRANOMES Across Group

The following are given for the tetranome A, B, A1, B1:

- a. inverse frequency listing of the highest 100 tetranomes
- b. repeat rate
- c. chi-squared statistics
- d. total sample sizes

## 5. MONOGRAMS

- a. A listing of monograms comprising 50% of the total sample, sorted in inverse frequency order
- b. The same as above, except sorted by telecode number
- c. Statistics:

- monogram frequencies
  - percentages
  - total percentage displayed
  - unique monograms displayed
  - unique monograms processed
  - total of frequencies displayed
  - total sample size

- \*d. A complete inverse frequency listing of all unique monograms in the entire sample, together with:

- the frequency distribution
  - percentage
  - the cumulative percentage
  - the Chinese graphic characters
  - number of unique monograms
  - repeat rate
  - total frequency displayed
  - total number of unique groups displayed

- \*e. The same as above, only sorted by telecode number

## 6. DIGROUP STUDIES

- a. A listing of chained digroups comprising 15% of the sample, sorted in inverse frequency order
- b. The same as above, but sorted by telecode number
- c. Statistics:

- frequency distribution
  - percentage
  - Chinese graphic characters
  - general English meanings



# TOP SECRET UMBRA

repeat rate  
chi square statistic  
number of unique digroups displayed  
sample size

- \*d. An inverse frequency listing of all digroups occurring three or more times, using the entire sample as the data base. Also given are the frequencies and percentages.
- \*e. The same as above, but sorted by telecode number.

## 7. TRIGROUP STUDIES

- a. A listing of chained trigroups comprising 5% of the sample, sorted in inverse frequency order.
- b. Same as above, but sorted by telecode number.
- c. Statistics:
  - frequency distribution
  - percentage
  - repeat rate
  - unique trigroups displayed
  - total frequency displayed
  - sample size

\*d. An inverse frequency sort of trigroups occurring two or more times in the entire sample, with the frequency and percentage.

\*e. A telecode number sort of the above.

## \*8. SENTENCE BEGINNINGS AND ENDINGS

- a. An inverse frequency listing of 75% of those monogroups appearing at the beginning of sentences

Also given: the frequency distribution  
percentages  
Chinese graphic characters  
general English meaning  
total frequency displayed  
total unique groups displayed

b. Same as above, but with sentence endings.

## \*9. PUNCTUATION

- a. Total number of commas in entire file and percentage.

**TOP SECRET UMBRA**

- b. Total number of periods in entire file and percentage.
- c. The new total sample size, including punctuation (not included in other runs, because punctuation is represented by symbols rather than 4-digit groups).

## 10. 5-5 WINDOW INDEX

On each of the eight categories individually.

The above statistics were developed both on the eight individual subject categories and on the entire file (ALL SUBJECTS), except where the \* appears. The \* indicates the statistics were done on the entire file only, and not on the individual categories.

George Sing, B4, has promised a large file of newspaper articles which will also be processed along these lines. This will add another dimension to the data base, making this project wider in scope.

	STC FILE DATA BASE
--	--------------------

<u>Categories</u>	<u>Number of 4-Digit STC Groups Excluding Punctuation</u>
1. FICTION	537,122
a. Drama	
b. Literary Essays	
c. Novels	
d. Novellas	
e. Short Stories	
2. ESSAYS	135,911
a. Biography	
b. Literary Criticism	
c. Educational Essays	
d. Political Essays	
e. Social Essays	
3. HISTORY	60,579
a. Sociology	
b. Ancient History	
c. Intellectual History	
d. Modern History	
4. COMMUNIST IDEOLOGY	104,996
5. KMT IDEOLOGY	20,997

# TOP SECRET UMBRA

6.	LANGUAGE	
	a. Literary Policy	70.326
	b. Language and Rhetoric	
	c. Language Standardization	
7.	JOURNALISM	22,955
	a. Editorial Journalism	
	b. Reporting Journalism	
8.	PHILOSOPHY	44,027
	a. Philosophy	
	b. Literary Criticism	
9.	(LAW)	(5,000)
10.	(ARCHEOLOGY)	(2,800)

ALL SUBJECTS (includes all of the above categories  
1,003,194)

The last two categories (law and archeology), were included in the ALL SUBJECTS runs, but omitted in the processing of individual categories because of the small volumes in the categories, and unusual subject content.

Therefore the data base represents 10 general subject categories, composed of 25 subcategories.



**TOP SECRET UMBRA****SEEDLINGS**

--- SO LONG! IT'S BEEN GOOD TO KNOW YOU.

By decree of Gen. Herbert E. Wolff, DDO, publication of *DRAGON SEEDS* will cease with this issue. We are grateful to all of you whose volunteer efforts made it a publication B could be proud of. Please submit future articles for publication to: *CRYPTOLOG*, Pl.

\*\*\*

---The B4TDT is looking for a general term which would describe the functions of a "meaning digit," "ø-select system," and other devices which permit the user of a code or code chart to modify, change, truncate, expand or limit the meaning or plain-text value of a code group. Send your suggestion to Betty Dunn, B4TDT. If we get a good one, we will send it on to Mr. Callimahos for possible inclusion in the Basic Cryptologic Glossary.

\*\*\*

---OMNIBUS

OMNIBUS is a network of computers being developed as an enhancement of the existing WARSAW system. The network will consist of a dual processor DEC System 10,

and eleven or more PDP-11s. The DEC-10 will control the network and interface with other Agency computers through a PDP-11. Other PDP-11s will control the CRTs and GRAPHICS communications.

The dual processor DEC-10 configuration is currently comprised of 96K of core memory with paging hardware, one swapping drum, two discs and sixteen CRT terminals. Future expansion is expected to reach 256K of core, four drums and twelve discs.

Version 5.06A of the standard DEC-10 monitor is the current operating system. This is a time sharing monitor that provides service for up to 35 time sharing or batch users.

The PDP-11 systems in OMNIBUS are 16K minicomputers using the RSX-11A Operating System. This is a real time executive that can handle a multi-programming environment yet utilizes only 2-5K of core memory. Other major features of this system include modular design, fixed priority scheduling and time dependent task initiation.

For information concerning the OMNIBUS operating system contact Aaron Engel or Pete Wyatt, C433, X4286.

\*\*\*

**TOP SECRET UMBRA**

# TOP SECRET UMBRA

---Misplaced during departure from the TDLA, a small volume of poems in Korean with English translations. Please notify Minnie M. Kenny, x5078 if found.

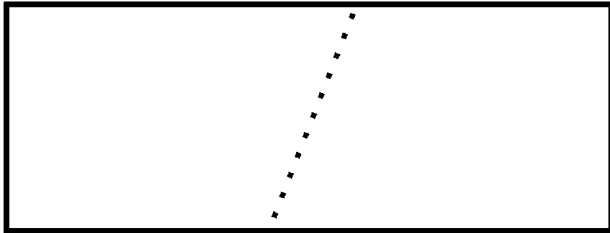
\*\*\*

## ---B CRYPT SEMINARS

To help us working analysts break out of our "target" boxes we plan an open-ended series of informal and informative technical seminars so that we can all learn more about B Group cryptosystems and operations. Each meeting will be an audience-participation, show-and-tell session of one fairly limited B crypt or crypt-related subject. It will be led by whoever knows most about the problem, usually the analyst who is now working it.

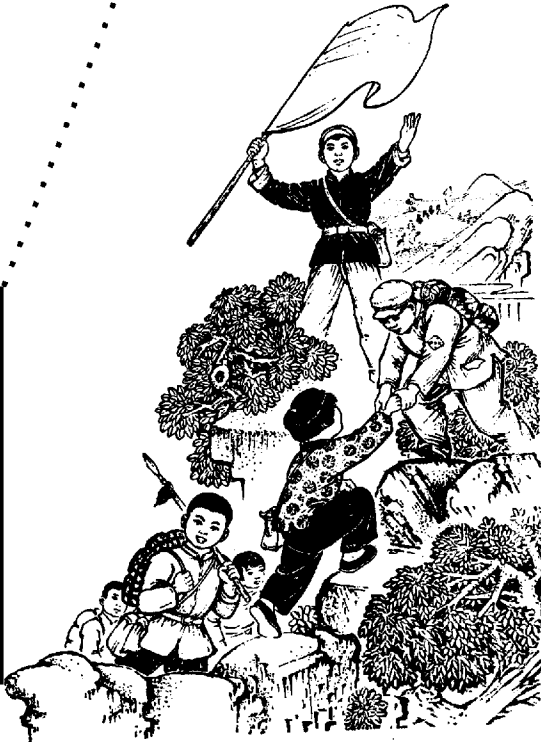
We will try to hold one seminar each month but will not bind ourselves to a rigid schedule.

The following subject have been suggested:



Crypt Documentation  
Calligraphy

Suggestions of topics and group leaders are welcome at any time. Bill Mau of B43 has agreed to lead a session on [redacted] to start off the B crypt seminars. Time and place for the meeting will be announced later.



# TOP SECRET UMBRA

---The muezzin moored, the tocsin tinkled, and the faithful flocked to the Call. Verily a select population! The now 235 Dundee members for the last 19 years have formed the hard core of soft-hearted, pliable, versatile technicians nurtured in the arcane mysteries of a noble art in the finest traditions of the giants of yesteryear. (Wa-we-woo, we were almost carried away there!) Eyes dimmed, if not from the ravages of time, at least from the emotional strain of our awesome responsibilities. But juubun is enough (in Japanese that is).

Wednesday, 12 June, was the Eighth Annual Reunion of the Dundee Society, held as usual in the Ballroom of the Fort Meade Officers Club. The festivities began at 1115 with convivial tinkling of glasses.

As was the Dundee custom, mystery guests of suitable noble birth and station, General Lew Allen Jr. and Benson K. Buffham, were present to receive Honorary Membership.

\*\*\*

*The Chinese word for 'crisis' contains two characters - one of them means 'opportunity'*

危 机

\*\*\*

## ---CACP Basic Requirement for a Computer Program

For a computer program to be accepted by the CACP either as meeting the basic requirement or for additional points:

1. It must serve a cryptologic purpose related to the cryptanalysis or exploitation of operational encrypted traffic.
2. It must work.
3. It must give evidence that the aspirant has a good appreciation of the role computers should play in supporting cryptologic activity.
4. It must demonstrate a professional attitude on the part of the aspirant by exhibiting a number of the functions generally incorporated in a computer program, by showing originality of purpose or technique, and by performing a complete task.

(Note: Originality, technique and a display of basic programming knowledge count more than amount of output, number of lines of coding and degree of operational usage. For instance full credit would be given to an original one-line APL program that printed "yes" or "no" on a one-shot pass if it accepted C/A data, wrung it out, tallied, tested and computed an important statistic. This is in contrast to a program which might serve a vital operational function by simply converting 26-letter

# TOP SECRET UMBRA

sequences to sequences of L's and R's denoting the halves of a typewriter keyboard, but which certainly doesn't demonstrate professionalism.)

Programs written as exercises in programming courses are not acceptable. Compartmented programs will be accepted for evaluation.

\*\*\*

## ---Teaching Opportunities

A note from Eliot Sohmer, Head of the Computer Science Department, E21, passes on the information that the National Cryptologic School has some unique opportunities for professionals who wish to sharpen their skills by teaching.

What many NSA employees don't realize is that you *do not* have to be permanently employed at the School to teach. This presents an opportunity for an employee to teach in any area of his specialty.

If you think that you might be interested in teaching a class or running a seminar, call Jack Leonard, E1, x8027 or Eliot Sohmer, E21, X8555.

\*\*\*

## ---PROFESSIONALIZATION NOTES NEW CRITERIA FOR CSAs

Have you heard that a New Criteria for Computer Systems Professionalization has been

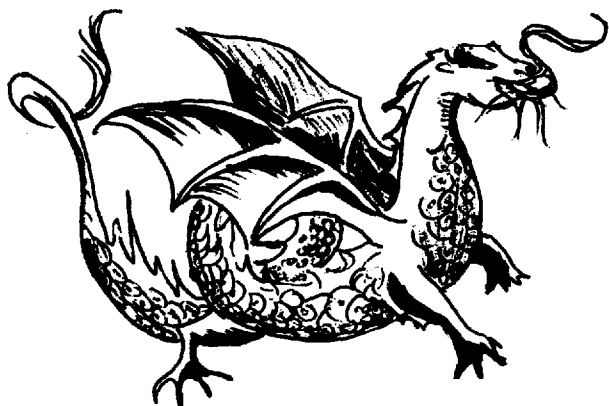
approved and published? It became effective 1 January 1974 and should have reached your element by the time you read this.

If you have not been certified as yet, it will affect you. If you submitted your PQR prior to 1 January 1974, you will be rated under the Old Criteria unless you make a request, in writing, to be rated under the New. Those rated under the Old Criteria will continue to maintain all the points awarded under the Old Criteria but will earn additional points and fall under the New Criteria effective 1 January 1975, if they have not been professionalized prior to that time. This grace period is covered in a memo that was approved by the CSCP and ADPS.

The general effect of the New Criteria is to require a technical paper from all aspirants (not just Interns) and to require the Interns to pass the same examination that all other aspirants must pass. It also places more emphasis on current training and computer related education, because this field is so dynamic that computers studied ten years ago are not nearly as relevant as computers studied today.

Detailed information can be obtained from the Data Systems Career Panel.

\*\*\*

**TOP SECRET UMBRA**

ASK  
THE  
DRAGON  
LADY

Dear Dragon Lady:

While we're still discussing the linguist at NSA, I feel a few words should be said about his training, especially where the minor tongues are concerned. In that regard, I'd like to pass on some points made by Prof. Carleton Hodge of Indiana University in a paper titled "Pedagogic Responses to Linguistic Stimuli" presented at the Georgetown Round Table. (March 1973).

Thorough cultural study should accompany the linguistic study of little-known languages.

Experiments have been conducted in which some students beginning the study of foreign languages were given drill in speaking from the beginning while others went through a "pre-speech phase" in which for eight weeks they developed only comprehension ability without attempting speech. It was found, that when the latter group was taught to speak, pronunciation, as well as comprehension, was better than that of the former group.

Fully structured texts are needed so that points of grammar are understood before they are used rather than explained afterward.

Robert F. Kreinheder

\*\*\*\*\*

*What can be done for the linguists?  
Theirs is not gain, but loss,  
For they only talk to each other  
And nobody talks to the boss.*

*Anonymous (alias Marian Griggs)*

50

**TOP SECRET UMBRA**



# TOP SECRET UMBRA

Dear Dragon Lady:

In the issue dated March 1974, the article titled "B Signals Lab Capabilities and Mission" was erroneously listed as being written by Mr. Robert Earles. The article was originally written as a memorandum to be distributed down to the branch level throughout B. Somehow in the transformation from memorandum to "Dragon Seeds" article, the name of the correct drafter became somewhat of a mystery. So that the record might be set straight, the undersigned recognized the need for such an item, discussed the idea with the Deputy Chief of B43 and wrote the article as it appeared in your March 1974 issue

Donald K. Autry

\*\*\*\*

*"This wise man has indeed a healthy mind";  
He sees an aberration as it is  
And for that reason never will be ill."  
-- Lao Tzu*

\*\*\*\*

Dear Dragon Lady:

Where can I get extra copies of the March 1974 issue of Dragon Seeds? Several of my G analyst friends would like copies of their own to use as RYE reference manuals.

Sonia Randall, H11

Dear Sonia:

Asking is receiving

\*\*\*\*

Dear Dragon Lady:

There should be some general diagnostic programs on the LODESTAR system.

Some interesting points:

Persons most familiar with the 6600-7600 systems will state that the inactive mode is not the most efficient way to use

# TOP SECRET UMBRA

these computers.

And, at least 1/2 of our cryptanalysis (in B) depend upon general diagnostic programs rather than specialized or interactive type programs.

Anyway, there's nothing to stop individual users from putting the general diagnostic programs in their workspaces.

The RAPID programs are in bad shape, and rewriting the most frequently used of these in BETA will correct the errors, as well as make them available on Burroughs 6700 and the 7600.

When and if these programs are rewritten, it will be done in as interactive a way as possible to cut down on output and machine time. (Eg. BIGSTET format rather than STET)  
So why not on LODESTAR and now?

Mary Ann Laslo

\*\*\*\*

Dear Mary Ann:

Will forward your query to C for resolution.

D. L.



\*\*\*\*

*A special word of thanks to Brenda Collins, Jackie Haislip, Helen Ferrone, and Jan Sanderson for their willing and able assistance in getting this last issue to press.*

# TOP SECRET UMBRA

## CONTRIBUTORS

DAN BUCKLEY has spent a year at [redacted] and three months at [redacted] on language related assignments since his last appearance in DRAGON SEEDS (The Ground Zero Approach to Language Analysis, Volume II, Nr 1 March 1973). He was certified by the Language Career Panel in March 1969 and by the SRA Panel in February 1972. He is currently assigned to the North Vietnamese Air Defense problem in B32.

JANE (BETTY) DUNN'S connection with SIGINT dates back to WWII and covers targets from Japanese Military to CHICOM [redacted] [redacted] with stops along the way for work on [redacted] European Satellite, and Vietnamese Communist cryptosystems. She holds a B.E. from Duquesne University and was prepared to teach French in Pennsylvania high schools before she was detoured to Arlington Hall. Betty is a certified cryptanalyst, a tutor for the CA Intern program, an E.E.O. counsellor, and most recently the Cryptanalysis Editor for the new magazine, Cryptolog. In the latest B reorganization, Betty was assigned to the B4 Technical Discipline Team.

BEE KENNARD, C522, graduated from the University of Texas with a B.A. in History and English. For seven years she served as an intelligence analyst with G2, U.S. Forces in Austria. In October 1959, she joined NSA and has since worked in the various area branches of C52. From 1967 to 1971, she worked with P2223 collocated information support group as the senior analyst on the Vietnam military problem. She is a professional Information Science Analyst and is currently writing articles on the new ideas and techniques in information services.

MARY ANN LASLO, B432, was graduated from Rosary Hill College, Buffalo, New York, in 1965, receiving a B.A. degree in Mathematics. She came to NSA in 1966 and entered the C/A Intern Program, which provided opportunities to work in A55, B45, G41, and G42. She received her certification as a mathematician in 1970 and as a cryptanalyst in 1973; and she has completed several requirements leading to certification as a crypto-mathematician. From 1969,

**TOP SECRET UMBRA**

to 1973 Mrs. Laslo was assigned to G91, where she did independent cryptanalytic research on the Peoples Republic of China [redacted] and functioned as a consultant in mathematics and statistics at Division level. Mrs. Laslo is now chief of the Chinese High Grade Cryptanalysis Team in B432.

JOHN J. MOLLICK, B25, studied Mandarin Chinese at Yale University Institute of Far Eastern Languages in 1955-56 and then served as intercept operator, voice transcriber, and traffic analyst with the USAFSS in Korea until 1958. His NSA (and B) civilian service stretches from 1959 to the present, punctuated by an academic year (1966-67) of advanced Chinese area and language studies at the U.S. Foreign Service Institute in Taichung, Taiwan. Mr. Mollick is certified in the fields of Language (Chinese) and Special Research. He was a frequent contributor of Chinese language articles to the Quarterly Review for Linguists. His present position is Chief of the PRC Documentation and On-Line Processing Branch, B253.

GEORGE NEWHOUSE, B21, received his B.A. in Business Administration from the University of Maryland in 1970 and is now completing work for his M.B.A. at the University of Hawaii. Since he came on duty with the Agency in 1963, he has worked on various B problems as a traffic analyst and reporter. A certified Special Research Analyst and Traffic Analyst, George now serves as the technical representative at USM-3 in Okinawa.

JOE REID retired 30 June 1974, ending a SIGINT career that dates back to WWII when he was a U.S. Navy intercept operator. His assignments at NSA and predecessor agencies covered Soviet low-, medium-, and high-grade cryptosystems, and included 15 years experience on Soviet and Chinese Communist data systems.

PAUL SAVAGEAUX has worked in B21 since 1965, after having completed a tour as Intelligence Analyst at Pacific Army Headquarters in Honolulu the previous year. He spent eight years on the [redacted] problem and is currently assigned to B21's Term Reporting Team which is writing a history of the PLA [redacted]. Paul graduated from the University of Massachusetts in 1961. He is a certified Special Research Analyst.

GOOD  
BYE...

