JUN 72

~~TOP SECRET~~

National Security Agency

Fort George G. Meade, Maryland

DRAGON SEEDS

~~APPENDED DOCUMENTS CONTAIN~~
~~CODEWORD MATERIAL~~

~~TOP SECRET~~

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

PL 86-36/50 USC 3605

DRAGON SEEDS

Publisher

DONALD E. MC COWN, CHIEF B03

Managing Editor	Executive Editor
Minnie M. Kenny	Robert S. Benjamin
Feature Editor Richard V. Curtin	Biographical Editor Jane Dunn
Rewrite Editor Victor Tanner	Education Editor Marian L. Reed

Special Interest Editor
Ray F. Lynch

Composition

Helen Ferrone
Lorna Selby

PRESS CORPS

B11	Carolyn Y. Brown	B42	Peggy Barnhill
B12	Philip J. Gallagher	B43	Mary Ann Laslo
B21	Gary Stone	B44	Jack L. Thomas
B31	Jack Spencer	B45	John E. Uzarek
	Thomas M. Beall	B5	Paul M. Hoagberg
B32	Jean Gilligan	B62	[redacted]
B33	Louis Ambrosia	B63	Allen L. Gilbert
B34	Thomas L. Wood	B63	William Eley
B41	James W. Schmidt		

Vol. 1
Nr. 3

June 1972

TABLE OF CONTENTS

CHIEFS OF STAFF

E. LEIGH SAWYER
CHIEF, B02

DONALD E. MCCOWN
CHIEF, B03

DELMAR C. LANG
CHIEF, B04

JOHN B. CALLAHAN
CHIEF, B05

"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

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

E. 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

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

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.

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.

* * * *

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

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

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

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

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 [redacted] 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.

* * * * * *

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.

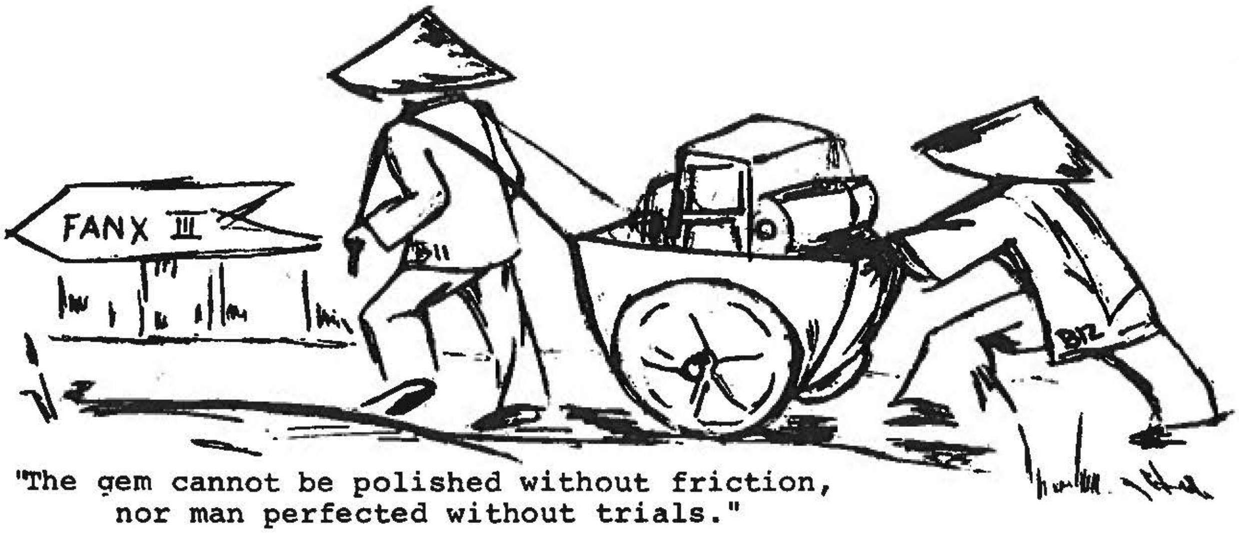
4. Determining possible methods of attack as a means of associating homogeneous intercept and performing follow-on analysis: In making this determination, we must ask, "What would we do if the old tried and proven analytic techniques and aids were no longer available?" A definitive answer to this question 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.

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."

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 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).

* * * *

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 [redacted]

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,

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. [redacted]

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 <u>any</u> 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 <u>every</u> 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

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 cryptanalytic 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 cryptanalytic 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.

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 — **Rotor development table (2 wds).**

   _ _ _ ○ _ _ _ _ _ ○ ○ _ _ _

2. R A H R I C H E Y — **Order of superiority in a set of wheels driven by notch rings.**

   _ ○ _ _ ○ _ _ _ _

3. A L L P A L E R — **Pair of wires of equal length.**

   _ _ ○ _ _ ○ _ _

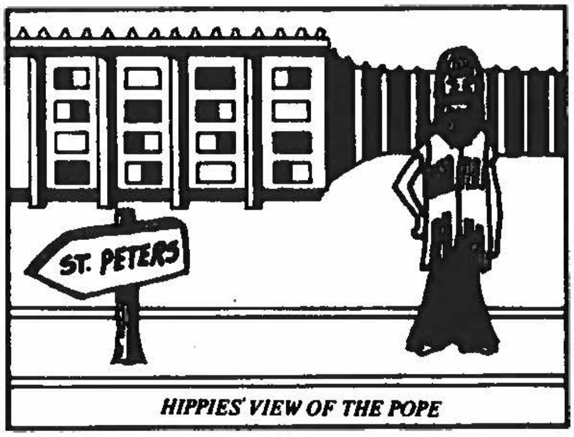
4. N O F I T I T O N A C A R — **Encipherment process involving encipherment, disassociation, and further encipherment.**

   _ _ _ _ ○ _ _ _ _ _ _ _ ○

5. D E A L S P E N T — **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.



HIPPIES' VIEW OF THE POPE

Print CRYPTOANSWER here

_ _ _ _ _   _ _ _ _ _ _

Answer on page 31

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

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., *nilijiumiza*, "I hurt myself," from -*umia*, "to be hurt."

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."

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.

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

STUDY OF ZFK MESSAGE ACTIVITY, CHICOM [redacted]

by Kenneth Miller, B433

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

[redacted]

****

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
```

VIETNAMESE COMMUNIST TACTICAL COMINT OPERATIONS ~~(SCW)~~

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

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 [redacted]

[redacted]

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

----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] in an effort to furnish the [redacted] 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.

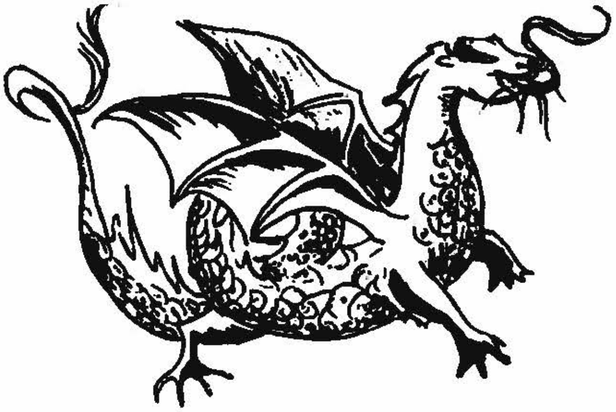
****

----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.

****



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, 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 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."

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

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, bookbreaker, 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] 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

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 CY-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.

Remember!

It's classified