MAR 72

Pl
Mr. L. D. Callimahos

~~TOP SECRET~~

National Security Agency

Fort George G. Meade, Maryland

DRAGON SEEDS

THIS DOCUMENT CONTAINS 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

~~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

Biographical Editor
Jane Dunne

Rewrite Editor
Victor Tanner

Education Editor
Marian L. Reed

Special Interest Editor
Ray F. Lynch

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 [redacted]

B63 Jean C. Smith

B64 Allen L. Gilbert

B65 William Bley

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Vol. 1
Nr. 2

March 1972

TABLE OF CONTENTS

~~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

A 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-

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 [redacted] 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 crypt-analytically 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.

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 practices of the target. In other words, I believe that the cryptanalyst must look to the communications center for his salvation. 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

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.

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] has provided me with the opporutnity 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] 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.

CHICOM DEVELOPMENT [redacted] AND THE AG-22

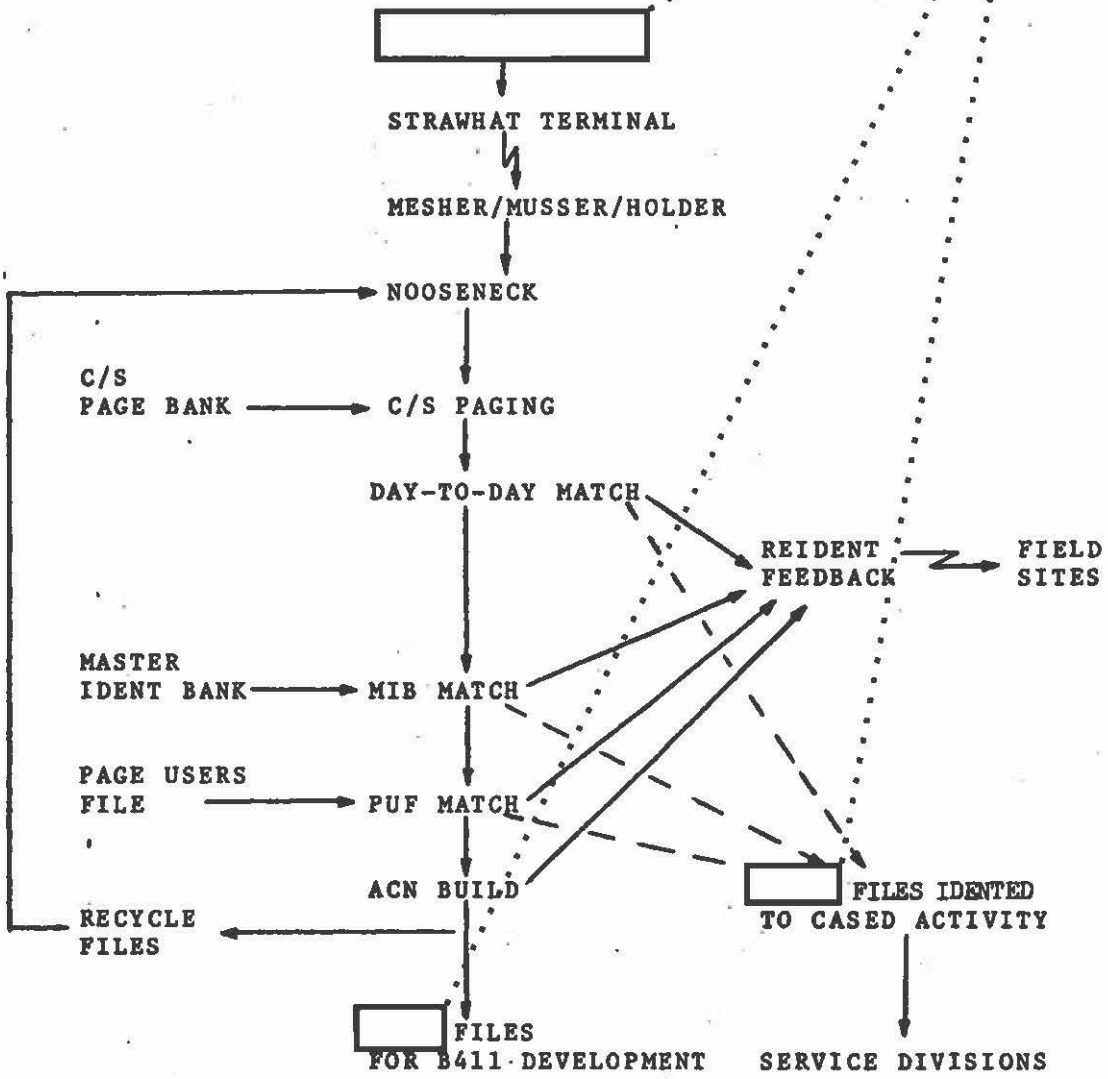
by Philip Remsberg

How do the AG-22 and the machine programs designed to process its output affect the handling of CHICOM Development [redacted] 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 interoept 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 [redacted] 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 [redacted] conversationally referred to as a [redacted] ditter. HOMESPUN raw traffic comprises approximately [redacted] 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 [redacted] identification programs devised for use with the AG-22 input.

To illustrate, let us assume that, at 1509 Okinawa time, [redacted] activity assigned to an intercept position at [redacted] is inactive and that under HOMESPUN the intercept operator is copying a [redacted] 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 [redacted] ditter, is soon picked up and delivered to the local terminal of the STRAWHAT data link for transmission to Ft. Meade. At the

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



NSA STRAWHAT receiving terminal, the data is recorded on a magnetic tape (MESHER/MUSSER/HOLDER) along with other [redacted] 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 [redacted] ditter by machine follows the callsign paging routine. The [redacted] ditter under consideration was copied at [redacted] The same activity, however was copied at other far eastern sites and identified. Assume that USM-48 had identified the activity as [redacted] Except for possible garbles, the callsigns for both intercepts should be the same. A routine of NOOSENECK compares the callsigns of the [redacted] 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 2-5Ø rule states that at least 2 callsigns and no less than 5Ø% 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 [redacted] 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 [redacted] 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 [redacted] 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 preceeding 5-day period as well as fixed callsigns of CHICOM [redacted] and other activities along with associated case notations. Callsign matches must meet the 2-5Ø rule for an acceptable identification. Comparison

with the callsigns in MIB increases the chances of an identification in the event that the [redacted] 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 [redacted] 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 2-5Ø rule still applies but in relationship to the number of callsigns on a page; i.e., at least 2 callsigns or 5Ø% 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 [redacted] 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 2-5Ø rule for a callsign page but no case notation equation for that page exists in PUF.

Activities that remain [redacted] ditters may eventually be assigned a 2-day continuity ACN or otherwise identified by the day-to-day or MIB match because [redacted] 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 [redacted] 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 [redacted] intercept that has been

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.

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

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).

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

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,

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 thepast. 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, [redacted], 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

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,

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 36Ø/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.

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
   _ _ _ _ O _ _ _ _ _
   Helpful format for recovery of transposition systems.

2. T W I T S
   _ _ _ O _
   RYE program which decrypts single or double transposition.

3. T R A I N I S O N P O S T
   _ _ _ _ O _ _ _ _ _ _ _ O _
   Cryptosystem which does not change the identities of the plaintext characters.

4. O D D L E O
   _ _ O _ O _
   The only RYE program which will produce a crenelated diagram.

5. A R A G M A N
   _ _ _ O _ _ _
   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

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 hav managerial responsibility will not necessarily possess manageme skills. The National Security Agency, in acknowledgement of th provides a broad managerial development program supplying educa tion 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 whereever 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.

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 expediture. 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] 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

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.

STRATEGIC IMPORTANCE OF SHENYANG MILITARY REGION

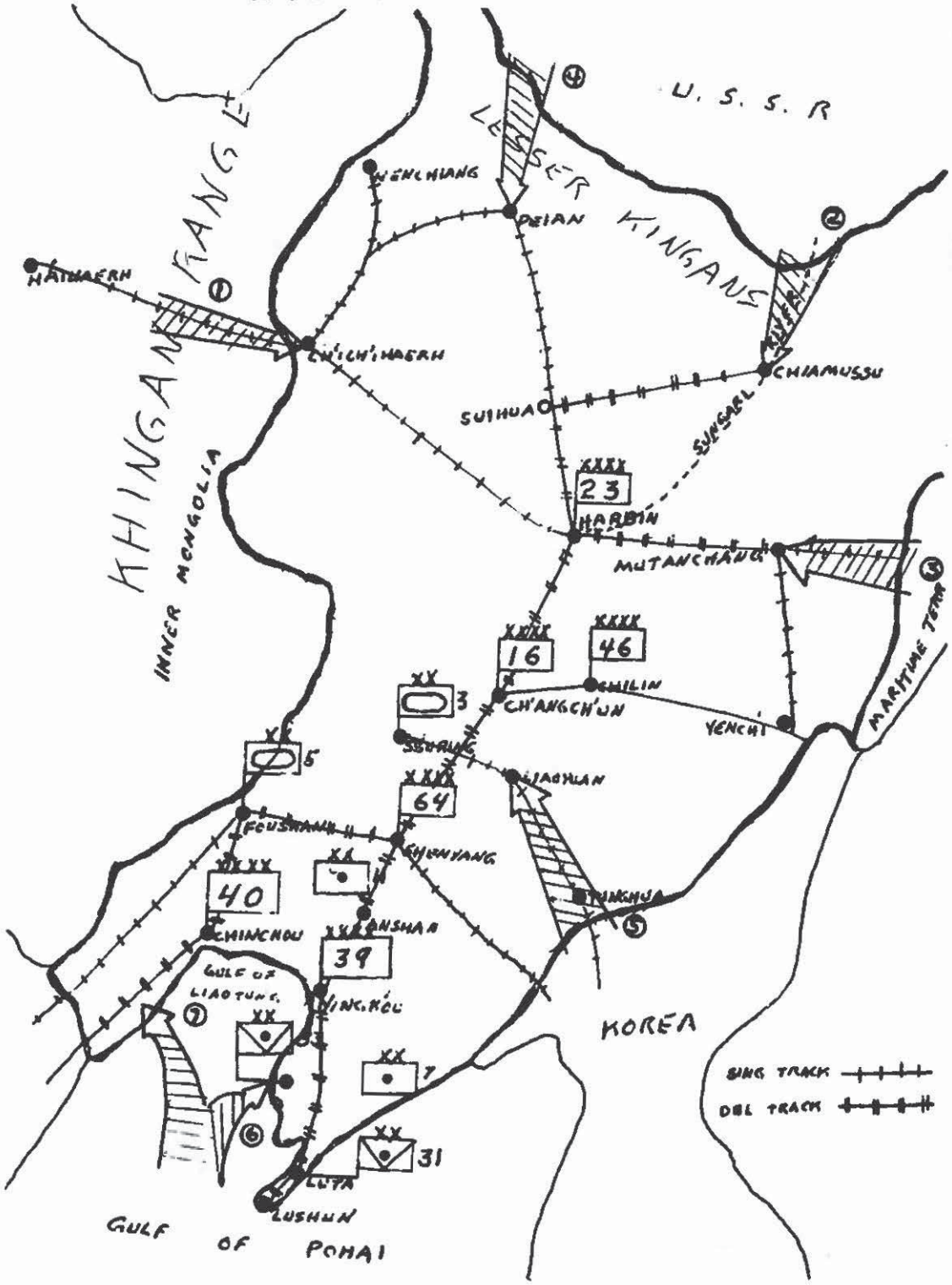
by Claire D. Smith, B205

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


U. S. S. R
KHINGAN
LESSER KINGAN
HSINGAN
INNER MONGOLIA
HAILAERH
MANCHOULI
WENCHIANG
PEIAN
CH'ICH'IHAERH
SUIHUA
CHIAMUSSU
SUNGARI
XXXX 23
HARBIN
MUTANCHIANG
XXXX 16
XXXX 46
CHILIN
CH'ANGCH'UN
YENCHI
MARITIME
XX 3
SHUANG
XX 5
LIAOYUAN
XXXX 64
FOUSHAN
CHENYANG
XXXX 40
XX
TUNGHUA
CHIANCHOU
XXX ANSHAN
39
GULF OF LIAOTUNG
YINGKOU
KOREA
XX 7
XX 31
LUTA
LUSHUN
GULF OF POHAI
SING TRACK
DBL TRACK

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.

* * *

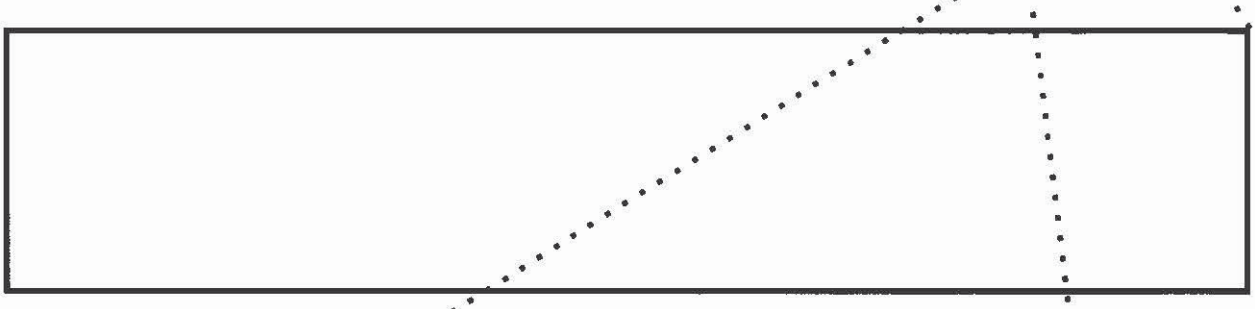
"Who spilled the ink on the Code room floor?"

"DAH-DAH DI-DIT"

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



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.

LETTER FROM PLEIKU

by Tom Glenn, B61

During late 1967 while I was on TDY to Plekiu, 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 O5ERS,

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.

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.

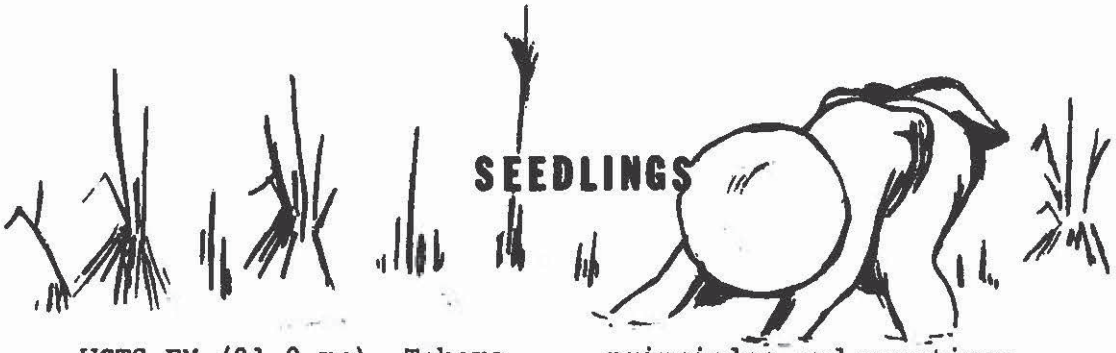
And there's always that feel in the air--
Just knowing the VC are there--
Armed with such trifles as punjis and rifles,
With claymores and dum-dums to spare.

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 tasts run.
If one of your vices is permanent crises,
Your search for Utopia is done.



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

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 first-hand 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.

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.

***

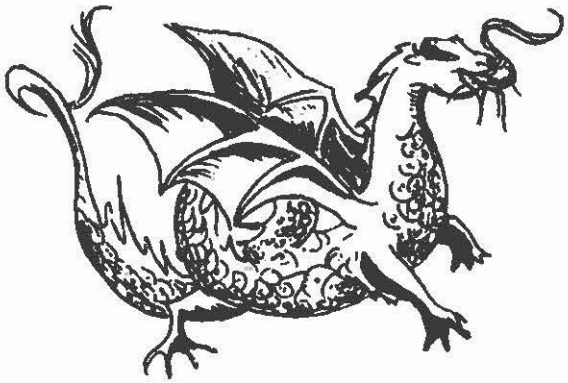
Your attention is called to the 26-week television series of film classics to be shown on WETA, Channel 26, every Friday night at 8:30. These films--most of them foreign--carry the original soundtracks, and this is an exceptional opportunity to hear ten foreign languages "in action" without leaving your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



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

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

****

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

****

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

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.)

*****

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, bililteral substitution cipher is defined as 'a substitution cipher in which the ciphertext units are pairs of characters.' Not a

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.

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.

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.

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.

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!!"

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.)

Shhhhhhhhhh. . .

it's classified!