Doc ID: 6708419

~~TOP SECRET~~

National Security Agency

Fort George G. Meade, Maryland

DRAGON SEEDS

SEPTEMBER 1972

~~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

DRAGON SEEDS

Publisher

DONALD E. MC COWN, CHIEF B03

Managing Editor	Executive Editor
Minnie M. Kenny	Robert S. Benjamin
Feature Editor	Biographical Editor
Richard V. Curtin	Jane Dunn
Rewrite Editor	Education Editor
Victor Tanner	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	
B33	Louis Ambrosia	B63	George S. Patterson
B34	Thomas L. Wood	B63	William Eley
B41	James W. Schmidt		

Doc ID: 6708419

DRAGON SEEDS

Vol. 1
Nr. 4

September 1972

TABLE OF CONTENTS

B OFFICE CHIEFS

DONALD A. REED
Chief, B1

MICHIE TILLIE
Chief, B2

COL JOHN E. KENNEDY
Chief, B3

ROBERT A. HIGHBARGER
Chief, B4

STEPHEN J. O'TOOLE
Chief, B5

DONALD C. JACKSON
Chief, B6

"INDEED THE WISE MAN'S OFFICE

IS TO WORK BY BEING STILL;

HE TEACHES NOT BY SPEECH

BUT BY ACCOMPLISHMENT;

HE DOES FOR EVERYTHING,

NEGLECTING NONE;

THEIR LIFE HE GIVES TO ALL,

POSSESSING NONE;

AND WHAT HE BRINGS TO PASS

DEPENDS ON NO ONE ELSE."

        - LAO TZU

聖人

是 以 聖 人
處 無 為 之 事
行 不 言 之 教
萬 物 作 焉 而 不 辭
生 而 不 有 為 而 不 恃
功 成 而 弗 居
夫 惟 弗 居 是 以 不 去

        老 子

1

DONALD A. REED
Chief, B1

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

****

MICHIE F. TILLEY
Chief, B2

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

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

2

JOHN E. KENNEDY, COL, USAF
Chief, B3

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

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

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

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

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

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

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

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

* * * *

ROBERT A. HIGHBARGER
Chief, B4

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

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

* * * *

STEPHEN J. O'TOOLE
Chief, B5

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

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

DON C. JACKSON
Chief, B6

Dr. Jackson began his cryptologic career in 1953 as an Ensign in the U.S. Navy, working on the Soviet [ ] problem at Arlington Hall. He served in various Agency and field positions in a military capacity until 1957, including a tour as Officer-in-Charge of the Naval Security Group Detachment assigned to the Taiwan Defense Command and the U.S. 7th Fleet.
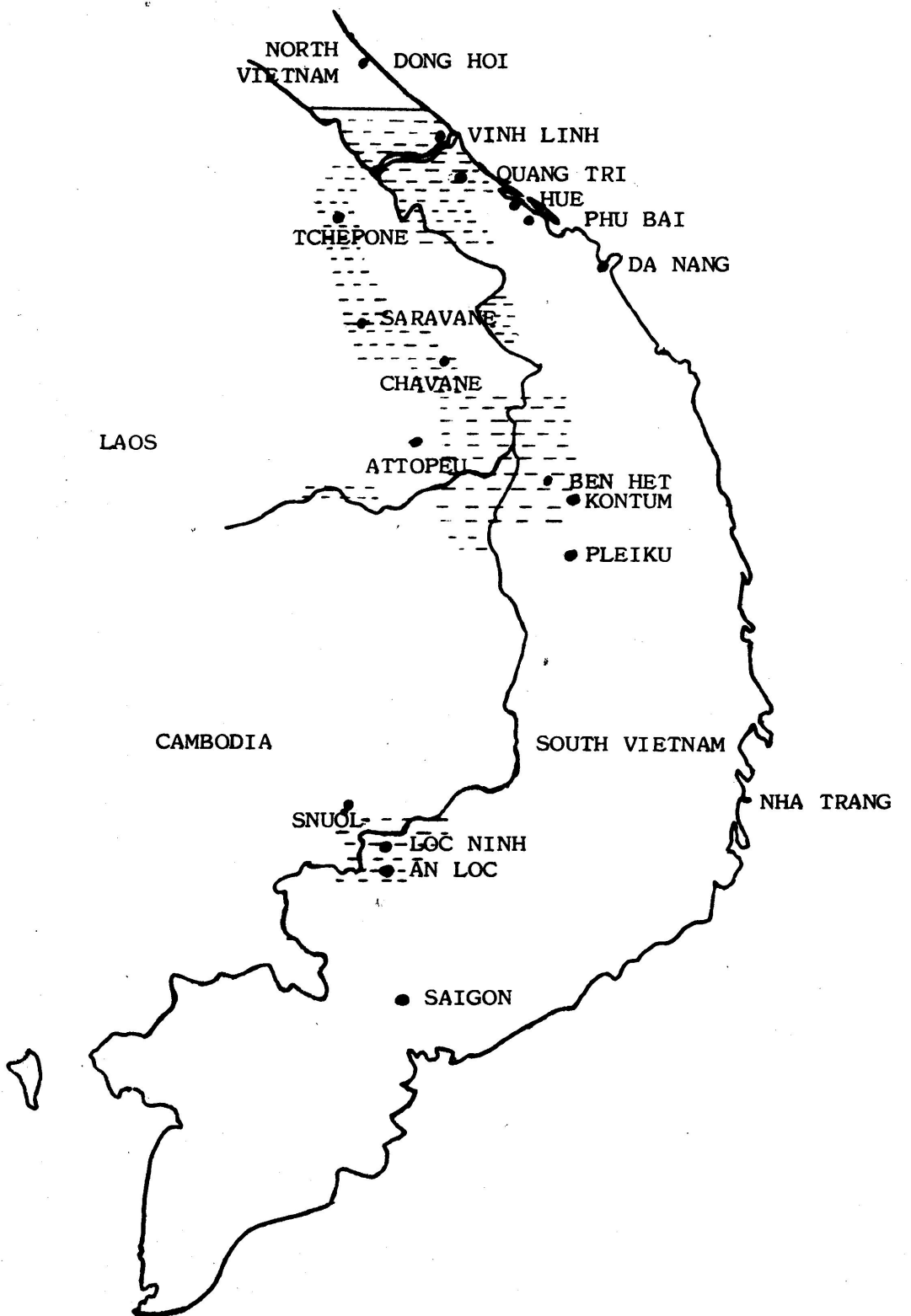
From 1957 to June 1961, he held various Agency assignments including Branch Chief positions for the Chinese [ ] Military problems. In July 1961, he became Chief of the Production Organization's resource programming staff, during which time the CCP was born. In 1964, Dr. Jackson was awarded an NSA Fellowship to attend George Washington University, where he completed requirements for the Doctorate degree.

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

****

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

NORTH
VIETNAM   • DONG HOI

VINH LINH

QUANG TRI
HUE
PHU BAI

TCHEPONE

DA NANG

• SARAVANE

CHAVANE

LAOS

ATTOPEU
• BEN HET
• KONTUM

• PLEIKU

CAMBODIA   SOUTH VIETNAM

NHA TRANG

SNUOL
• LOC NINH
• AN LOC

• SAIGON

Tactical areas
of operation for
NVA armor units

THINGS THAT GO CLANK IN THE NIGHT
          by Mike Hricik, B61

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

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

MEDIUM TANK T-54A

- CHARACTERISTICS -

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

8

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

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

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

AMPHIBIOUS TANK PT-76 (MODEL 2)

- CHARACTERISTICS -

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

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

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

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

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

TOP SECRET UMBRA

SIGINT AND AUTOMATIC DATA PROCESSING
by staff writers

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

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

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

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

TOP SECRET UMBRA

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

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

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

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

<p style="text-align:center">* * * *</p>

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

SEADEV--MECHANIZATION FOR T/A DEVELOPMENT
                                        Allen L. Gilbert, B63

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

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

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

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

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

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

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

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. **L E G F R O N D S**
   _ _ _ _Q_Q_ _

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

2. **T R U E P E A R**
   _ _Q_Q_ _ _

   Grille window.

3. **S H I P R O O M**
   _ _ _ _ _ _ _Q

   A sequence which has the same pattern as another sequence.

4. **P O E T W O R D A C T**
   _Q_ _Q_Q_ _ _ _

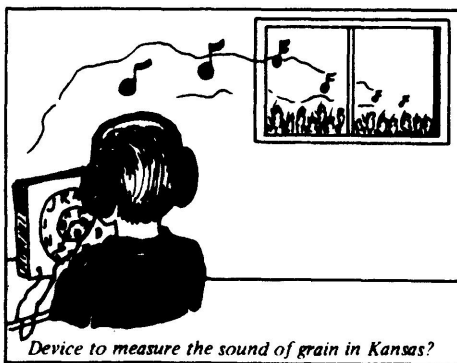   Requires both an enciphering and deciphering device.

5. **D R Y O M E N S**
   _ _Q_ _Q_ _

   RYE program which tests for monome-dinome substitution.

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

Print **CRYPTOANSWER** here

_ _ _ _ _ _ _ _ _

Device to measure the sound of grain in Kansas?

Answers on page 29

THE OPEN DOOR

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

-The Concept of Dragon Seeds

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

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

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

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

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

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

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

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

~~TOP SECRET UMBRA~~

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

Most indigenous languages of B12 [   ] employ what are often termed exotic writing systems. Characters which are bizarre to Western eyes are written in various combinations and juxtapositions to form syllables, of which tone indicators are a part. Unlike the Roman or Cyrillic alphabets, whose letters are written in consecutive order, characters of these languages ([   ]) are written in irregular patterns with some characters written above or below others: Since the number of characters involved is also larger, unique Morse equivalents must be used in some languages when communicating. Barred letters are used by collection personnel to represent the unique Morse characters. Some languages have no standardized method for spelling plain text in communications, but employ cipher equivalents instead.
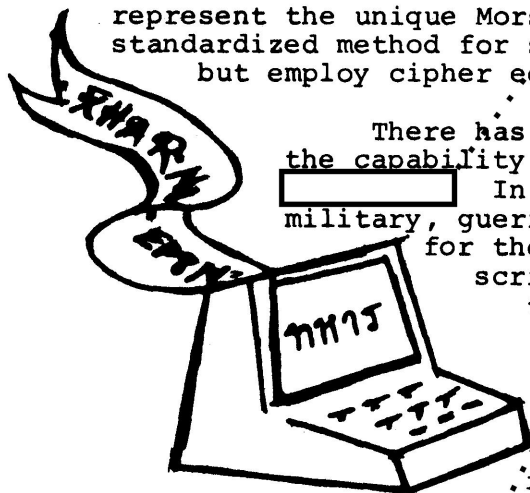
There has long been an interest in developing the capability for machine scripting of B12 [   ] In some countries, various entities (e.g., military, guerrilla) now use different equivalents for the same language, making the common script representation very desirable. With the increasing reliance on machine-supported analysis and machine decryption of cipher messages, there has been an increasing need for standard scripted output. Presently, the JUNGLE BOOK project is being launched to develop CAMINO-type machine dictionary files for B12 languages. This project should be a great help in alleviating the paucity of dictionaries and glossaries and should substantially assist efforts to exploit message texts. It is essential that published versions of these JUNGLE BOOK files employ native scripts. The use of script is also desirable for working aids and training materials so as to eliminate the confusion and difficulty that artificial representation entails.

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

~~TOP SECRET UMBRA~~

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

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

4060 Lao Output

ກຳແພງບະຄອນໃຫ້ໂຮງ
ຫະຫານຜູ່ບິງວຸ[ຄບານເບ

Lao Newsprint

20

A SOFTWARE APPROACH TO SCRIPT PROCESSING: THE HOW
by Ferdinand J. Reinke, Jr., B12

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

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

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

Burmese Newsprint

4060 Burmese Output

4060 Thai Output

Thai Newsprint

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

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

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

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

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

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

MACHINE-AIDED TRANSLATION
                    Norman Wild, B03

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

AUTOMATIC LOOK-UP

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

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

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

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

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

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

PRO	CON
1. Dictionary in machinable form is already available, or preparing one is desirable for other reasons--usually to print out a desk dictionary when no available one is satisfactory.	1. Machinable-form dictionary is not available and would not serve any additional purpose.
2. Input language is already in machinable form or has to be put in this form for other purposes. It may be that the input is available as a by-product of other operations.	2. Language would have to be punched or typed for this sole purpose.
3. Spelling of input language is consistent and compatible with the spelling on the dictionary tape.	3. Spelling is inconsistent and causes ambiguities and difficulty in equating to the form on the dictionary tape. The inconsistency could arise from ignorance, cryptographic constraints or options, lack of hard rules in the target language, lack of standard Romanization or Morse, etc.
4. Units of look-up are easy to find in the stream of text. Word-spacers are sent; a code group stands for a well defined word or phrase; etc.	4. Text is a stream of syllables or smaller units (down to letters) without word divisions, and words have to be found in the stream by unwieldy tests which are not always reliable.

PRO	CON
5. Base form is not changed much or at all by inflection.	5. Base form is changed drastically by inflection.
6. Translators are comparatively untrained and inexperienced and are slowed down considerably by lack of vocabulary.	6. Translators are familiar with common vocabulary and have difficulty only with advanced translation problems which an automatic look-up would not help.
7. Much vocabulary consists of technical terms with neat English equivalents.	7. Translation problem does not lie in the basic meaning of the word but in the best rendering in varying context.
8. There is much need for "extra-linguistic" information such as latitude/longitude of placenames, brief descriptions of personalities, arbitrary standard translations, expansions of abbreviations, etc.	8. Vocabulary should be familiar to a linguist with a good "traditional" knowledge of the input language.
9. Large vocabulary is used because of subject matter (e.g., industrial, scientific).	9. Vocabulary is not larger than a translator can be expected to learn.
10. Volume of text is great enough to make the basic expenditure worthwhile.	10. Volumes are small and intermittent; time spent in preparing the system could not be repaid.
11. Translations are not required immediately; we can tolerate the delays in preparing material for machine and waiting for printouts.	11. Translations are required in a hurry; material cannot wait for batching or technical and administrative delays.

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

SEEDLINGS

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

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

Meritorious Civilian Service Award
      Oscar Steele, B63

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

****

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

****

----The National Cryptologic School is offering the pilot presentation of a computer-managed course in FORTRAN IV from 0800-1630 hours daily in Room A1B33, FANX II. There is no registration, scheduled classes, or credit given for the course. Students proceed at their own pace, but must finish the course within five weeks. Those completing the course will be permitted to take the final exam for MP-227 (FORTRAN Programming) and should they pass, will be registered and credited for completion of that course. Interested personnel should contact Mr. Gibbs or Mrs. Garlick on extension 8555.

****

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

****

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

27

~~TOP SECRET UMBRA~~

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

****

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

****

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

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

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

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

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

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

****

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

WIN is reaching out to you.
Contact Olive Bennett, P1, or Dee Zellers, M3, and WIN!

****

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

****

28

~~TOP SECRET UMBRA~~

Doc ID: 6708419

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

****

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

****

----Appearing next in the current monthly lecture series of the Crypto-Mathematics Institute held in the NSA auditorium at 0930 hours are:
    Ralph E. Walker, R5 - 5 Oct 72
        Uses of the Fournier
        Transform in Digital
        Signal Analysis
        (SECRET/CODEWORD)
    Charles W. Bostick, G4 -
        2 Nov 72
        Probe Vectors (SECRET)

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

****

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

****

```
ANSWERS TO CRYPTO-SCRAMBLE:

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

CRYPTOANSWER:   WHEATSTONE
```

ASK

THE

DRAGON

LADY

Dear Dragon Lady:

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

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

And Nang Ha.Nyan's:

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

                              JOHN S. LAWRENCE
                              Chief, P16

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

The Dragon Lady humbly suggests that when trying
to locate experts in the minor tongues of mainland
Southeast Asia, P16 not overlook the talents of the
Justin Morse family, one of the most durable missionary
families in the China-Burma Hump who after 51 years of
administering to tribes in the "Shangri-La" valleys at
the "top-of-the-world" are back in the United States
renewing ties with the Christian Church following
ouster from their adopted homeland by the Revolutionary
Government of the Union of Burma. Through educational
and medical as well as religious programs, Dr. Morse
and family earned the loyalty of Kachin, Naga, and
Khamti Shan tribesmen so much so that until 1965,
these same hill peoples frustrated the central
government's efforts to serve expulsion orders initiated
in 1961.

* * *

Dear Dragon Lady:

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

DONALD P. LENAHAN, B2

CONTRIBUTORS

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

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

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

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

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

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

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

REMEMBER....

IT'S CLASSIFIED!