~~TOP SECRET~~

National Security Agency

Fort George G. Meade, Maryland

MARCH 1973
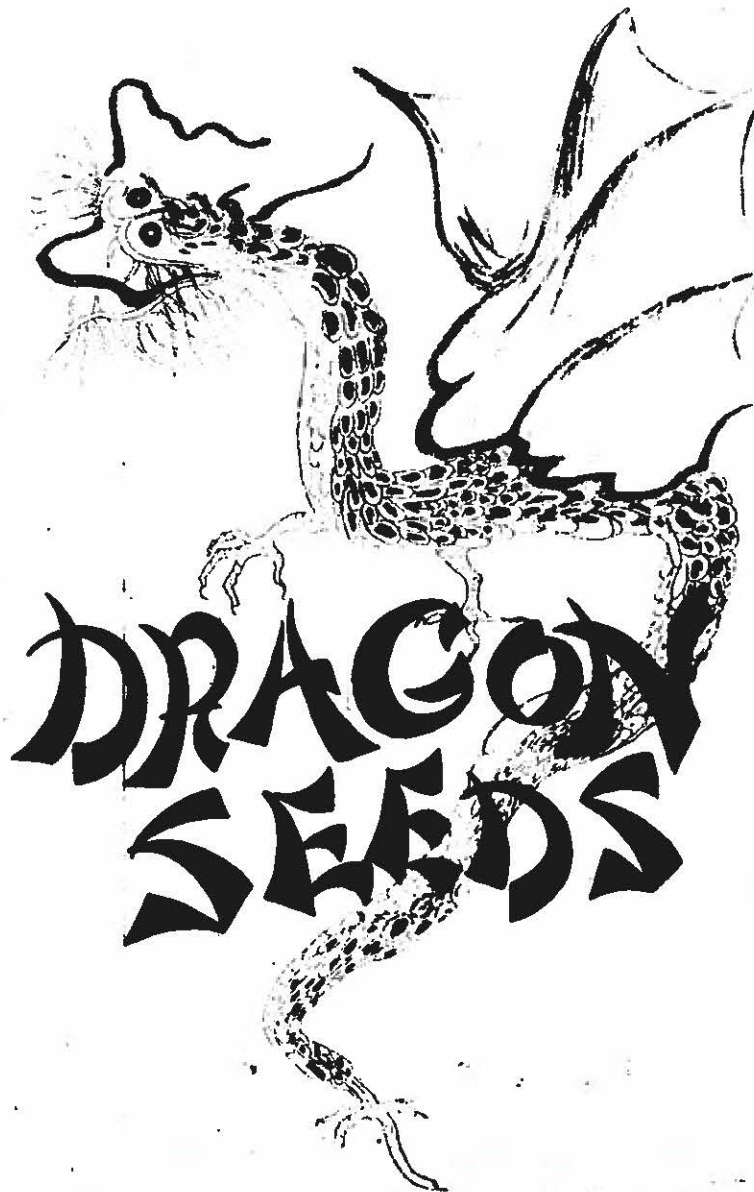
DRAGON SEEDS

This is *Dragon Seeds*.

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

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

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

Dragon Seeds is yours. May it grow with you.

                    The Editors

PL 86-36/50 USC 3605

DRAGON SEEDS

Publisher

DONALD E. MC COWN, CHIEF B03

Managing Editor   Executive Editor

  Minnie M. Kenny   Robert S. Benjamin

Feature Editor   Biographical Editor

  Richard V. Curtin   Jane Dunn

Rewrite Editor   Education Editor

  Victor Tanner   Marian L. Reed

Special Interest Editor

Ray F. Lynch

Composition
Composition

Helen Ferrone
Lorna Selby

PRESS CORPS

B11 Carolyn Y. Brown   B43 Mary Ann Laslo

B12 Philip J. Gallagher   B44 Jack L. Thomas

B2 Dee Ensey   B45 John C. Uzarek

B31 Jack Spencer   B5 Nancy Fournier

B32 Jean Gilligan   B61 [   ]

B33 Louis Ambrosia   B62 Edmond J. Guest

B34 Thomas L. Wood   B63 George S. Patterson

B41 James W. Schmidt   B63 William Eley

B42 Peggy Barnhill

PL 86-36/50 USC 3605

DRAGON SEEDS

VOL 2
NR 1

MARCH 1973

TABLE OF CONTENTS

NGỪNG BẮN

VIỆT NAM

THE JACK BUTCHER CASE
                    by William G. Flynn, B6

        On 24 March 1971, North Vietnamese ground forces shot
down a USAF OV-10 twin engine reconnaissance aircraft in the
Saravane area of Laos. The aircraft was piloted by 1st Lt
Jack M. Butcher, who was believed to have been injured in the
crash. He was, however, able to make a voice transmission
prior to his capture by enemy troops. Communist communications
of 25 March reported that an AAA battalion of Binh Tram 34
had shot down an OV-10 aircraft, and that they had captured
the pilot alive. Normally this would have been the end of it,
for SIGINT reflections of pilot captures were noted frequently
over the years. But this time it was not the end. It was
just the beginning of a saga in which SIGINT played a very
important role.

        One month later, on 26 April, a message was intercepted
which pertained to Lt Butcher, discussing the capture of an
American and describing him as an "intelligence type" (a term
used for OV-10 pilots, indicating visual reconnaissance).
Butcher had apparently received injuries during the crash.
This was indicated when a Rear Services element reported that
the American POW had "fully recovered" and preparations were
being made to transport him north through the Rear Services
system. His captors were instructed to send him "up" quickly
so that he could be interrogated. Apparently he had not been
questioned since his capture because no one in that area spoke
English.

        On 7 May, a commo-liaison station of Binh Tram 14 was
instructed to prepare to receive the "pirate POW" who was
being escorted by two infantry cadre of Binh Tram 34. The
stations were cautioned to be extremely vigilant in handling
the prisoner because he was a "die-hard"--apparently meaning
that they were having difficulty handling him.

        Sometime during the next two days, while being transported
north, Lt Butcher escaped, thus starting a series of events
that was unprecedented in the history of SIGINT support to
Search and Rescue (SAR) efforts. The message that triggered a
massive recovery effort was intercepted on 9 May and revealed
that "a lieutenant, an OV-10 pilot, being brought to the rear
had escaped due to our negligence." The message described the

lieutenant as "a spy" and "very dangerous" and further stipulated that if he was not captured, "he may cause damage to our entire system." When this message was received by the SIGINT Support Group for the Special Operations Group of MACV, the Joint Personnel Recovery Center (JPRC) was notified immediately. The JPRC commenced a check of OV-10 pilots known to have been downed in that area and confirmed that the prisoner referred to in the message had to be Lt Butcher. Lt Butcher's escape, evasion and recovery plan was then reviewed and a determination was made as to his probable direction of travel in his attempt to be rescued.

The following day, another intercepted message gave a description of the escaped POW and notified all units to be on the alert. Lt Butcher was described by the Hq 559th Transportation Group as still in uniform and wearing boots. Shoes were generally the first thing to be taken from a prisoner. This then indicated that he had been giving his captors trouble and had not accepted the fact that he was a prisoner of any permanency.

It was at this point that NSA became actively involved for the first time in a real-time recovery of a downed pilot. In addition to the normal reporting conducted by field elements, messages and technical back-up material concerning the plight of the American pilot were being forwarded to NSA via OPSCOMM immediately after intercept. This material was then reviewed and retranslated in an attempt to derive any possible additional information. I want to stress at this time that this action was not taken because we thought that the field stations were not doing an outstanding job--they were--but to emphasize the importance placed on the recovery of this pilot. For the next 20 days NSA had both linguists and technicians available on a 24-hour basis to assist in the recovery attempt.

The Communist search intensified. Binh Tram 33 instructed units to "motivate the specialized forces at the district" and to send someone down to the hamlets of Du Mong, Bang Xang Theng, and Hoi Hoi to discuss the matter with local force cadre and the troops of the Peoples Army at Tchepone. They were directed to "search until they find him." The fate of Lt Butcher was very much on the minds of the U.S. military commanders in South Vietnam. Captain Bill Coenen, USMC, chief of the SIGINT Support Group, was called upon to give a briefing on the Lt Butcher escape and recovery actions to General Abrams, CONUSMACV.
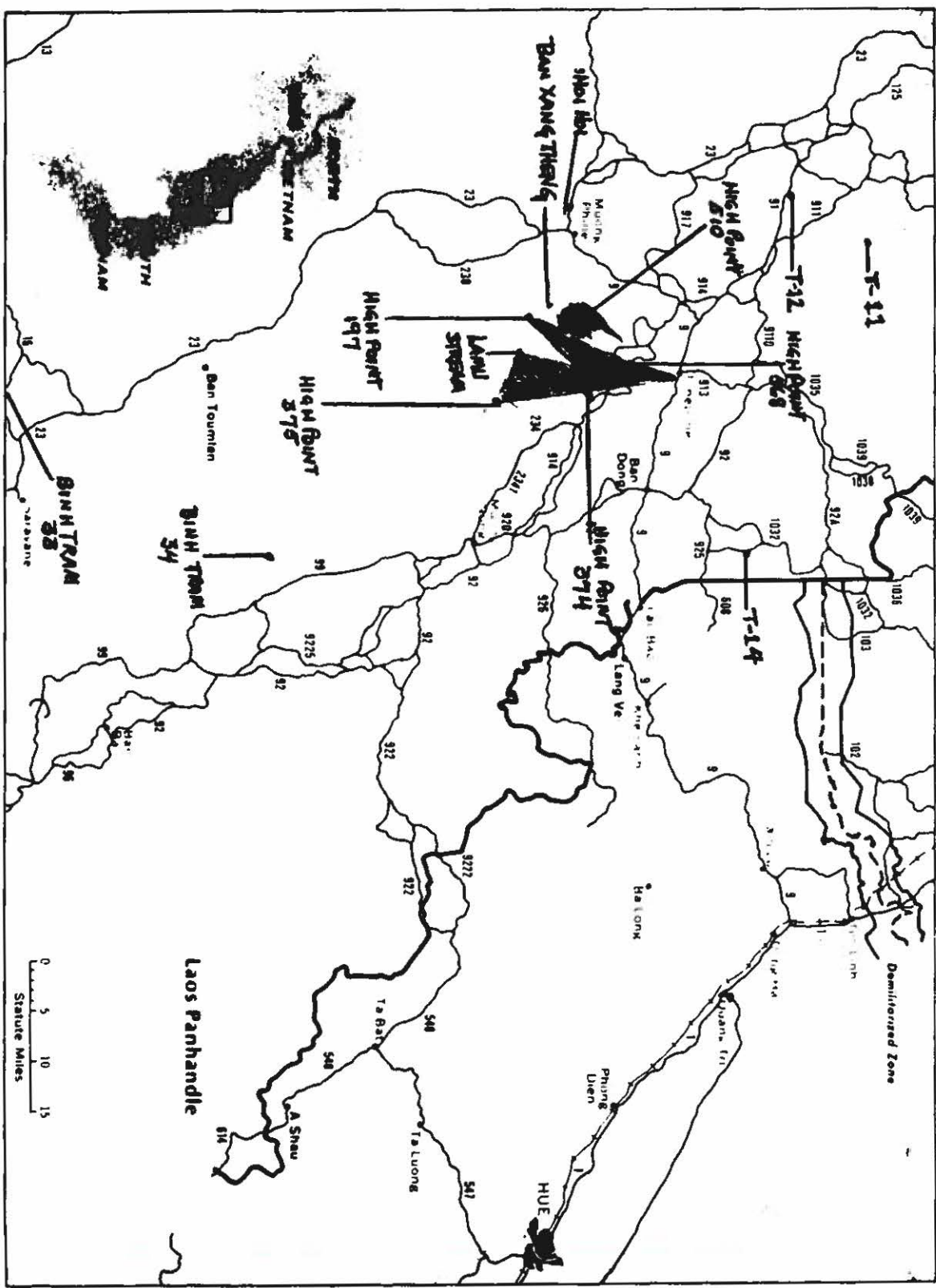
General Abrams ordered that all available assets be placed at the disposal of the Joint Personnel Recovery Center. The 7th Air Force made all its resources available, and moved helicopters to areas adjacent to the area in which it was believed that Lt Butcher would attempt to reach for recovery. In addition, daily photo missions were flown over this area for any sign of his whereabouts.

Communist entities in the Binh Tram 33 area continued to search for the escaped OV-10 pilot. On 13 May, it was reported that the Communists had formed two small teams which were searching in the area of High Point 568, High Point 197, and back to Tchepone. Upon arrival at Tchepone, they were instructed to search in small circles around the Lamu Stream and back to High Point 375 and eventually to an unspecified new storage area. Additional teams were ordered to investigate caves and streams in the vicinity of High Point 510 with great care. At this point, the Communists appeared to be sure that the pilot was still in the area of a new storage facility and concentrated their search in that area.

The search for Lt Butcher was one week old when, on 16 May, Communist units reported that on the previous day Allied helicopters had searched "area two" all day. Later the same day, another message disclosed that the "screeching owl," a derogatory term they were using to refer to Lt Butcher, was in "area one" and ordered that a sweep be carried out through that area. The search was to focus on "streams, rocky fields and cultivated fields," with particular attention on "high trees." One main search element was dispatched to the location where the "escaped enemy" was first seen.

There was no celebration of Ho Chi Minh's birthday for Communist forces in the Binh Tram 33 area because, as of 19 May, Lt Butcher was still at large and the search continued.

Lt Butcher had evaded his captors for about 10 days now, and yet, with all the Allied assets dedicated to his recovery, we still had been unable to rescue him. The time had now come to take a calculated risk. Aircraft equipped with loudspeakers were flown over the area we knew the Communist forces were searching. They attempted to contact Lt Butcher by broadcasting to him, using prearranged information contained in his escape, evasion and recovery plan, in an attempt to establish a rendezvous point for his extraction. The question at this

4

point was, would this compromise our SIGINT effort, or would the Communists merely surmise that Lt Butcher had been able to contact Allied forces. Whatever the thoughts of the Communists were, we will probably never know. But one fact is sure, we did not lose our intelligence collection from these units.

The broadcasting did not go unnoticed by the Communists, because on 20 May the Combat Operations Section of Binh Tram 33 reported that an OV-10 had used a loudspeaker to contact the pilot by secret means in areas one and two. As a result of this action, Communist forces sent out three search teams to form an ambush; but their efforts were in vain, since a later message revealed that the OV-10 pilot was still loose in the area. Another insight into the dilemma of the Communist forces searching for Lt Butcher was their concern, expressed by Binh Tram 33, over the possibility that civilians were assisting the pilot. It was suggested that a "proselyting team" be sent into the area to determine if civilians were hiding the POW.

Lt Butcher was probably recaptured by the Communists on 26 May after about seventeen days of evasion and living off the countryside. On 27 May, a dispatch from the Military Movement Section contained information concerning the northward movement of an American POW who was very stubborn, had escaped once, and had to be tied up. The report listed the prisoner's height as 1.8 meters and reported his name to be "BOOTS SOW," an apparent transliteration for Butcher. It was also reported that the American was white, had three broken teeth, and was wearing a black shirt, underwear, and long military trousers. Of interest is that in this instance no mention was made of his "high boots." Apparently the Communists had learned their lesson.

A few weeks ago, when the names of 10 POWs held in Laos were handed over to Allied authorities, Lt Jack M. Butcher's name was on that list. For a great many of us, this news had deep personal meaning. Hopefully, another chapter in the Jack Butcher case can be written at a later date, giving his side of the story.

REBELS IN THAILAND
        by Geoffrey Wood, B12

     Since taking up arms against the established government in
1965, Thai insurgents have slowly and steadily grown in number
and effectiveness, their activity marked by ever expanding use
of modern weapons and skillful guerrilla tactics with one
puzzling exception

Communism in Thailand

     At least as early as 1920, the Bangkok Chinese community
was sending funds to support Communist activities in both China
and India, and agents from those countries were busily soliciting
funds and talking of future revolution in Asia as an inevitable
consequence of the Soviet revolution. Small cells were estab-
lished, chiefly among students and members of the Chinese
community in Bangkok. In the late 1920s, Nguyen Ai Quoc (Ho Chi
Minh), disguised as a Buddhist monk, spent several months in
Thailand propagandizing the Vietnamese colony and establishing
a Communist youth organization. Later, many of these youths
became leaders in the Hanoi regime. Activity among the Thai
themselves was minimal, and Communism was generally regarded by
Thai officials as a foreign import without much appeal to the
generally contented and racially homogeneous Thai. In an
effort to divest the movement of its foreign--particularly
Chinese--flavor, the Communist Party of Thailand (CPT) was
founded in 1942, but its failure to dominate the World War II
Free Thai anti-Japanese movement, as well as its inability to
generate an active insurgency at the war's end (the only South-
east Asian Communist party that failed to do so), attest to
the Party's weakness and its lack of appeal to the Thai.

     Foreign influence and support continued, with Communist
China training exiles who provided leadership in the CPT.
During the late 1950s and early 1960s, North Vietnamese agents
active among Vietnamese refugees in Thailand helped to set up
the insurgency which was soon to follow. Arrangements were
probably made at this time for training of Thai Communist
recruits in North Vietnam and in Communist-controlled areas of
Laos.

6

Open rebellion began in 1965, before adequate foundations were fully laid. This premature action was probably taken at the urging of the Chinese and North Vietnamese to divert U.S. attention and resources from Vietnam and Laos, and perhaps to discourage the Thai government from more active participation in the Indochina war. The insurgents' decision to take up arms was announced from China by both Radio Peking and the Voice of the People of Thailand (located near Kunming, in Yunnan Province). Peking's announcement of Communist plans for Thailand suggests that China had a significant role in formulating the decision.

Insurgency Now

With fewer than 6,500 effectives in a population of 35 million and only about 1,000 CPT members, the insurgent movement does not now pose a threat to the regime. The government continues, however, to be troubled by its activities in remote areas where central authority is weak or non-existent.

The insurgency differs significantly from one region of the country to another. In the far South, where some 1,400 men are under arms, the insurgency is unusual; it is neither under the direction of the CPT nor directed against Thailand. The insurgents there are mainly ethnic Chinese, veterans of the Malayan insurgency of the 1950s and younger recruits. Their allegiance is to the Communist Party of Malaysia, and they are targeted primarily against Malaysia. Although they are not really a part of the Thai insurgent movement, they do pose a threat to governmental authority in the area.

In contrast to most of the country, the Northeast, the site of the first active insurgency, is plagued by drought and a chronically depressed economy. There are ethnic differences between the northeasterner and the central Thai; the region borders on the Laotian Panhandle and the northeasterner is culturally and linguistically more Lao than central Thai. The Communists play upon the cultural differences and on the desire of the villagers for a share in the apparent affluence of the central plain. In addition to sheltering about 2,200 insurgents, the Northeast is also the location of approximately 40,000 Vietnamese refugees who are ideologically loyal to Hanoi. They have not been closely involved in the insurgency, but the Thai view cooperation between the refugees and the insurgents as an ever present danger.

The insurgents in the Northeast are capable of low-level attacks on small Thai government units and installations. Poorly armed initially and without an adequate local support base, the insurgents were repulsed in early confrontations with the government. Since 1967, they have utilized more cautious tactics, avoiding direct confrontations with counter-insurgency forces, while improving the quality of their organization and the security of their village support bases. Recently, they have emphasized political indoctrination, establishment of village military units, and acquisition of more sophisticated small arms. They probably have influence over a population base of at least 100,000 people in the North-east.

Insurgency in the North, which broke out actively in 1967, was marked from the beginning by the participation of hill tribesmen, principally Meo, reportedly lead by Sino-Thai cadres. There has long been ill will between the ethnic Thai who live in the lowlands and the Meo tribesmen who resent efforts by the government to curtail their slash-and-burn agriculture, which damages the valuable teak forests. Recent attempts by the government to end the cultivation of opium have led to further friction, sale of opium being the sole source of cash for most of the hill people. Government losses in the North have always been heavier than in the Northeast, principally because the Meo had modern small arms and were fighting on their own rugged mountainous terrain. The Thai reacted to losses on occasion by indiscriminate bombing of mountain villages, which caused great resentment without inflicting any damage on the insurgents.

Because the insurgents were Meo and not Thai, the central government was not overly concerned by events in the North. Even the establishment of secure base areas in some of the rugged mountains bordering Laos did not appear to worry Bangkok. With evidence of Communist success in recruiting ethnic Thai villagers over the past two years, the government began to take a more serious view of the situation. Security forces mounted a so far unsuccessful effort to establish a presence in the mountains along the Laotian border.

The northern insurgents, avoiding major contacts except when the odds were in their favor, carried out intensive harass-ment of government operational bases in isolated areas and conducted effective ambushes along principal lines of communica-tion. Their tactics included coordinated attacks by groups of

8

up to one hundred men and well executed ambushes by large groups
employing mines and booby traps. They routinely used automatic
weapons (AK-47) against both personnel and helicopters, and
often used rocket launchers (M-79) in harassing ground elements.
Their arsenal included anti-personnel mines, especially a plastic
Soviet type, and in March 1971, they employed rocket-propelled
grenades to destroy an armored personnel carrier (APC), the
first confirmed insurgent use of this weapon. At the end of
March, an APC detonated an anti-tank mine, again the first use of
such a weapon in Thailand. The insurgents operated effectively
in platoon and company sized units.

Insurgent Communications

The skillful use of sophisticated weapons clearly reflects
the support given by the Chinese Communists and the North Viet-
namese.

There are numerous reported sightings of insurgent groups
carrying radios. Interrogations and inspection of captured
radios show most of these radios to be transistor receivers used
for listening to Communist propaganda broadcasts. No captured
rebel has ever admitted to insurgent use of radio communications,
although detailed descriptions have been obtained of courier
communications. A collateral report has furnished a wealth of
information on training given in North Vietnam and Communist
China to six insurgents. They trained for four years in the use
of radios for communicating. Nevertheless, the trainee who
defected had not seen or used a transmitter in the two years
between her return to Thailand and her defection in 1968. Other
collateral and interrogation reports document radio facilities
serving Pathet Lao support bases along the northern Thai border
with Laos. Messages are reportedly passed by courier to these
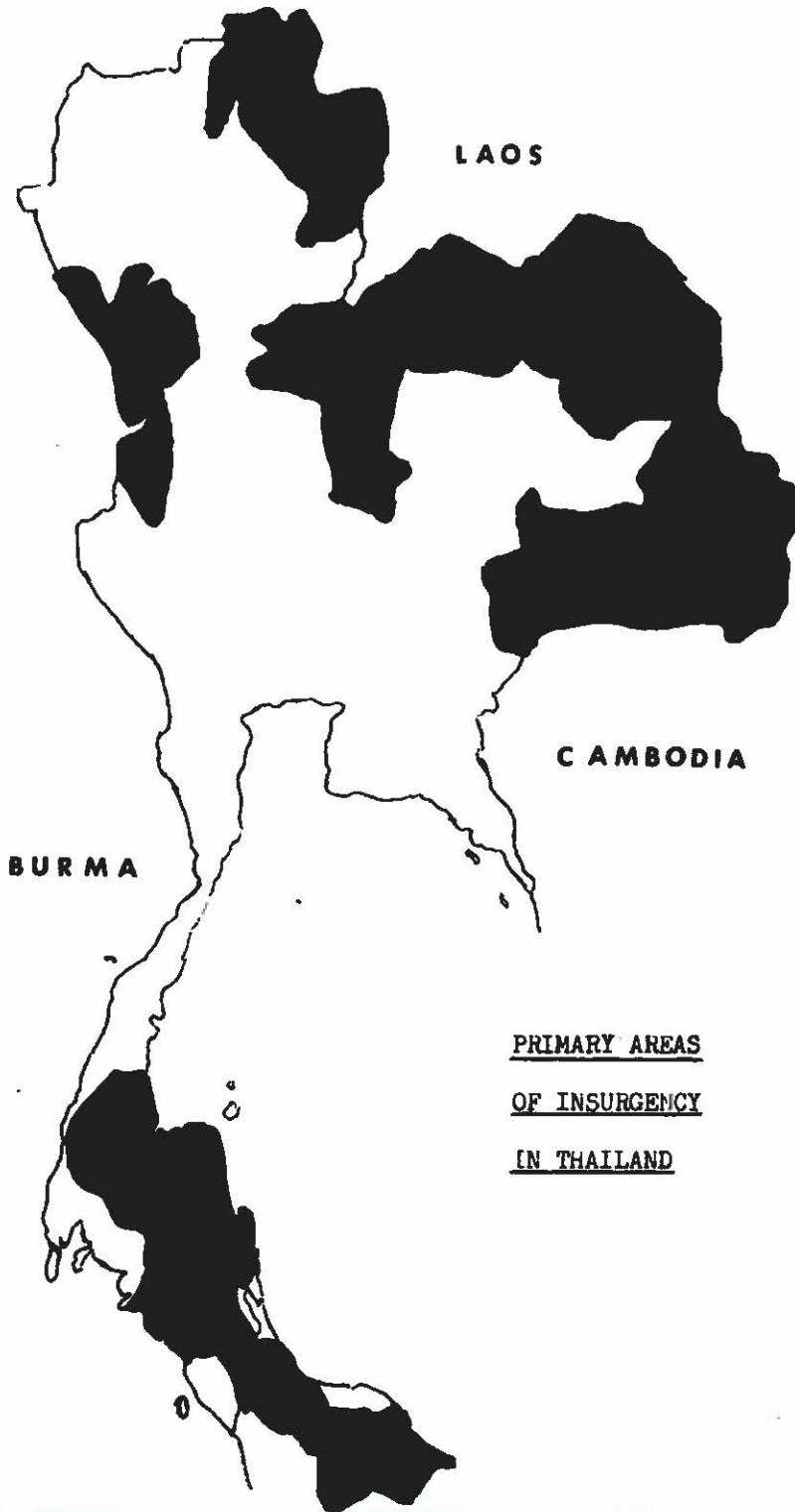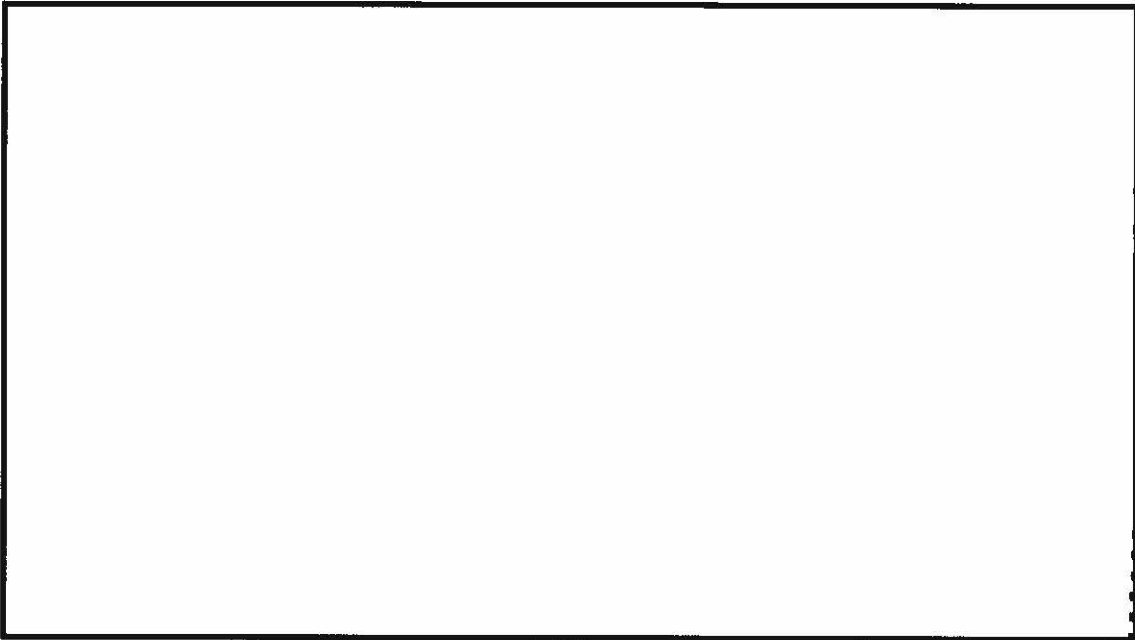facilities for relay to external addressees.
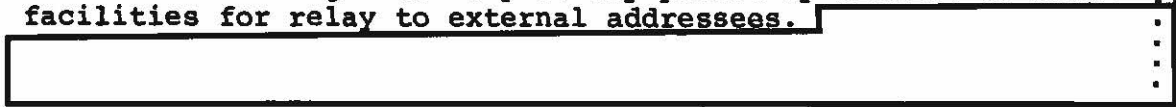
Radio Search Efforts

LAOS

CAMBODIA

BURMA

PRIMARY AREAS
OF INSURGENCY
IN THAILAND

10

There is conclusive evidence that both the Communist
Chinese and the North Vietnamese (to include their Laotian
clients, the Pathet Lao) actively support the insurgency in
Thailand. The support encompasses training at all levels,
material supply, the provision of safe havens, and high-level
policy guidance. Communications of these countries may well
be involved in support of the Thai insurgency, perhaps intelli-
gence, security, party, military, and press.
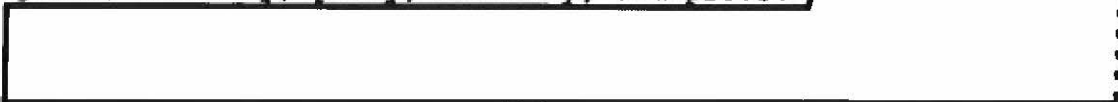
The insurgency, though small,
is growing, and insurgents have become increasingly sophisti-
cated in their tactics and employment of weapons, particularly
in North Thailand.

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

A GIST OF THE KOREAN SIGINT PROBLEM
                            by Richard S. Chun, B44

      Prior to June 25, 1950, when North Korean forces crossed
the 38th parallel, there was virtually no SIGINT effort on
North Korean communications. A U.S. Army Security Agency unit
(ASA Pacific) in Tokyo, Japan began intercepting North Korean
traffic. This effort was later augmented by a South Korean
intercept source (ROKN Group "M"). ASA Pacific established an
advanced element in Taegu, Korea in September, 1950; and by
mid-October, the 60th Signal Service Company (330th ASA
Company) from Fort Lewis, Washington, arrived in Pusan. Total
intercept was thus increased to 20 positions.

      The increased collection of North Korean communications
introduced a need for traffic analysts, cryptanalysts, and
linguists. There were no Korean linguists assigned to the
Armed Forces Security Agency (NSA). One male civilian who
had studied the language while hospitalized and a female
civilian of Korean descent, both employed by NSA, [ ]
[ ]   established the first Korean
language unit. [ ]
[ ]
The unit was augmented when reserve officers with previous
Korean language background were recalled to active duty; and
the Army Language School (DLI/W) at Monterey, California
assisted by accelerating its training of U.S. military personnel
in the Korean language. Meanwhile, two U.S. Army officers of
Korean ancestry, stationed as instructors at the Army Language
School, were assigned to the Army Security Agency and trans-
ferred to ASA Pacific, Tokyo. They were later joined by several
NSA linguists. (One of the instructors was LTC Youn P. Kim--
probably the greatest single contributor to the North and South
Korean SIGINT effort.) Complicating the shortage of Korean
linguists was the almost total lack of suitable Korean
dictionaries and knowledge of North Korean military and technical
terminology. A file of terminology appearing in North Korean
military communications was compiled. Definitions of terms
were determined by context and by reference to Japanese and
Chinese dictionaries. The file was supplemented by data from
prisoner of war interrogations, conducted by the two ASA
officers, and by captured North Korean documents obtained through
various U.S. military sources.

Much cryptanalytic success was achieved early in the war, and NSA and field personnel gleaned highly perishable intelligence information from decrypted messages. Most North Korean messages at this stage of the war were enciphered with low grade cryptosystems which changed frequently but remained unsophisticated in complexity. Voluminous end product translations produced during late 1950 and early 1951 were of great value to intelligence users. Messages emanating from high echelon North Korean sources revealed significant information concerning the capabilities and intentions of North Korean forces. Users for the United Nations forces considered this a valuable source of information. It has been estimated that approximately 85% of the total usable intelligence information during this period was furnished by cryptologic sources.

Exploitation of North Korean cryptosystems and translation of messages was hampered more by the sheer volume of messages than by the complexity of the systems themselves. Large volumes of significant message decryptions had to be published by a small work force. However, by the Spring of 1951, the cryptosystems became more sophisticated and exploitation became increasingly difficult. This was often attributed to the intervention of Soviet advisors who apparently became alarmed over the lack of communications security. Despite increased security efforts, U.S. cryptanalysts were successful until the fall of 1951, when North Korea first introduced "pad" encipherment. The percentage of exploitable messages dropped, less plaintext was used, and the overall intelligence furnished by SIGINT decreased.

Traffic analysis posed no problem during the hostilities. Most of the callsigns, frequencies, identifications, and locations of North Korean forces were recovered from decrypted messages. Following the truce, however, traffic analysis was a painstaking problem. Progress was finally made when North Korea began using ▢▢▢▢▢▢▢▢▢ Direction finding operations were unsuccessful primarily due to the rugged Korean terrains and equipment malfunctions associated with the mobile operation.

Non-military North Korean communications targets were first intercepted in 1952. Internal civil communications, which in many respects resembled our Western Union, produced plaintext messages passed among major North Korean cities and

industrial complexes. These messages contained a large variety
of subject matter ranging from personal messages to coal, lead,
zinc, and other mining statistics. In addition, order of battle
information was derived when these messages were passed among
members of the military forces.

Intercept of South Korean targets was initiated in June
1953, when South Korean President Syngman Rhee released approxi-
mately 25,000 prisoners without advising U.N. authorities.
South Korean military, navy, air, and police communications
were very closely monitored, particularly whenever President
Rhee threatened to take unilateral action against North Korea.
This threat action delayed the signing of the truce agreement
for at least thirty days, until July 1953.

Since open hostilities have ceased and the situation has
become static, North Korea continues her efforts to improve
communications security. There has been further sophistication
of cryptosystems and rigid adherence to communications security
procedures. The use of radio communications has decreased,
while the use of landlines and courier services has increased.

A SIGINT effort which began with North Korean forces
crossing the 38th parallel on 25 June 1950, and developed to
the point where valuable and useful intelligence resulted, has
finally, with the conclusion of the war, reverted to a quiet
peacetime problem. However, despite recent peaceful overtures
between North and South Koreans, the North Koreans remain a
well trained and well equipped military force with Chinese Red
volunteers sitting just across the Yalu River.

Not only does a SIGINT requirement exist today, but SIGINT
takes on a more significant role during peacetime situations
when communications security is at its peak. During periods
of open hostilities, the mobile situation tends to lessen
communications security and offers the SIGINT producer a variety
of intelligence sources.

東洋의 山

이한직

비쩍 마른 어깨가

抗議 하는 양 날카로운 것은

舍發 않고는 못 참는

애달픈 天稟을 타고난 까닭일께

다

激 한 噴火의 記憶을 지녔다

그 때는 어린 대로 심히 怒 해

볼수도 있었기때문이다.

植物들은 해마다 헛되히

뿌리를 받았으나

끝 내森林은 이루지못 하였다

지나치게 悽愴함을 겪고

나면

오히려 이렇게도 마음고요

해지는 것일까

THE HILL OF THE ORIENT

YI HAN-JIK

THAT MY BONY SHOULDERS ARE SHARP
AS IF IN PROTEST
PERHAPS IS FROM THAT IMPATIENT
TEMPER OF MINE
WHICH SEES AND MUST ACCUSE.
I CARRY MEMORIES OF VOLCANIC
VIOLENCE;
FOR THEN I WAS FREE TO BE FURIOUS.
MY PLANTS HAD ROOTS, IN VAIN,
EVERY YEAR
AND NEVER GREW TO BE A FOREST.
IS IT BECAUSE I HAVE WALKED
THROUGH TOO MANY CRUELTIES
THAT I AM IN SUCH QUIETUDE?
I HAVE NOW NOTHING TO INSIST UPON.
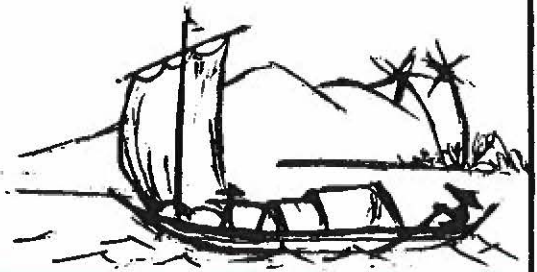
이제는 固執 하여야 할 아무
主張 도 없다

지금 山기슭에 "부주카" 砲가
震動 하고
共産主義者들어 낯설은
外國 말로 喊聲을
올린다
그리고 實로 믿을수없을만큼
손쉽게
쓰러저 죽은善意의 사람들
아 그러나 그무엇이 나쉬이고요
함을
깨들일 수 있으리오
눈을 꼭 감은채
나의表情은 그대로 얼어붙었나
보다
微 笑 아저 잊어버린
나는 東洋의 山이다

AT THE MOMENT
THE HILL-SIDES SHAKE FROM THE
    BAZOOKAS;
THE COMMUNISTS RAISE SHOUTING
    IN ALIEN TONGUES;
AND THOSE GOOD-WILLED PEOPLE
    HAVE FALLEN SO EASILY
THAT I CAN HARDLY BELIEVE IT.
BUT, NOTHING CAN DISTURB ME OR
    MY QUIET NOW.
WITH TIGHT CLOSED EYES,
THE ICE OF MY EXPRESSION FREEZES
    HARD.
I, WHO EVEN HAVE FORGOTTEN HOW
    TO SMILE,
AM THE HILL OF THE ORIENT.

        TRANSLATED BY KIM JONG-GIL

道

Transposition is.....

Our previous example of transposition involved a diagonal and blank cells. This is a simpler but still an intriguing version. Can you recover the key and the plain text?

```
E T N N S   C E T A H   L I I A A   I W R O X   E L E S T

H E E E E   L A A S I   C U T R B   E S V I F   S U A W H

B O Y R L   S D P D M   U D I S E   T O W M T   I Y Y V E

S S T F L   H P M U D   T N W R H   P S E L H   I S F O I

L O M C R   N U I V T   L T O C E   T E L N G   U S O E E

N N X M A   B T O A N   H T I O S   C I W N I   X I C N G

M L O T A   X F B P E   N H H E R   L O P E B   L E S E P

E R E E D   C E I E N   E I O N T   L S I E N   O I E R A

R I C O O   O T T O O   M A N U O   I T O X I   L T E L A

T O A V E   X O A I F   E Y A E N   O T O L P   M A B O M

X E A E N   O C E A X   A E F E A   U X L R T   N I O O Q

X N R T P   I R I R E   N E F E X   L T X T E   O N H I T

F O O U R   E H Q O O   H O R U C   G N X E O   P C O N D

R C R H D   B O U R N   I G K X N   M H O E V   T E S H T

R U T W D   E T N H I   N M L E D   E U R U A   C E D H A

I R O G E   T G S D M   B I A X L   T E T E V   E O A F B

M E X I Y   M E H H N   E C H S A   N N R A M   T P T E H

R W E C I   T C N T W   C X D D R   M N I R G   N W I T N

A Y E X C   E A G A F   F E W O L   X V W L D   E S O N S

D H M N R   E Q X A E   N A T I G
```

Solution in the next issue.

THE OPEN DOOR

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

-The Concept of Dragon Seeds

SIGINT SUPPORT ON THE ECONOMIC FRONT
by William Hunt, P2

When I was asked to write an article on SIGINT support to economics, it occurred to me that there was a feeling among certain personnel that the problem in NSA was something new. Most of us know that economic intelligence production in NSA is not new. I think it would be useful, though, to try to anticipate what changes in processing priorities will result from the statements of the United States Government regarding an increased emphasis on our economic posture, involving the placement of this country in a more competitive position vis-a-vis other major trading countries of the world and (a still more readily understandable consideration) the continued high value of our currency.

It is true that the emphasis in the past has been on military-type economics (which includes the production of weapons, weapon systems and hardware, the testing of new weapons, delivery of new weapons and related supplies to their national units and to foreign collaborating countries, etc.) and specifically on the ability of Communist Bloc countries to prepare for and sustain hostilities against the United States and its allies. It can be readily seen that almost any aspect of a country's economic status would contribute to the knowledge of its military capability. It can be concluded, therefore, that economic information from SIGINT has always been high on the mission of NSA. Priorities from time to time

have changed, depending on the requirement for this information
and the general resources available. Generally speaking,
priorities affect the scope of collection, the depth and detail
of analysis, and the frequency and timeliness of reporting.

In August of this year, G Group decided to take a look at
its readiness to respond to an increased interest in economic
SIGINT. Since G produces most of the non-military type of
economic SIGINT, and since this category is the most likely to
be affected by an increase in the priority of economic intelli-
gence, Chief, G Group established an "economic coordinator"
as an advisor to look into the whole of the G Group economic
SIGINT problem, including requirements, collection, processing,
and reporting, with a view to being in a position to respond
to any changes in the general G Group priorities system. A
study staff of up to six personnel was envisaged to undertake
this project. A basic charge to this staff was to study the
problem but not to become involved in operations; its activity
was to be confined to study--to probing the general problem
area and reporting on the ideal organization within G Group to
cope with the potentially increased emphasis on economic SIGINT,
if such should be required.

The writer and one additional intelligence analyst have been
studying this problem since August, and have just completed
an interim report on the status of G Group and some recommenda-
tions to improve the G posture to meet the anticipated challenge.

Considerable progress has also been made in the customer
community, including the rejuvenation and enlargement of the
USIB Economic Intelligence Committee and the establishment of a
sub-committee to deal with economic requirements. At this
writing, a new Assistant Secretary for Economic Affairs has been
named at the State Department (Mr. Casey), and Mr. Schultz,
Secretary of the Treasury, has been given responsibility for
over-all coordination of U.S. economic affairs.

With the exception of piecemeal, *ad hoc*, one-time require-
ments, no major SIGINT requirements demanding commensurate
resources have been levied on NSA beyond the normal and mostly
military-type economic requirements discussed above. Possibly
some reorientation of the priority and/or processing of existing
requirements will be forthcoming, and possibly there will be
totally new requirements with emphasis on specifics and on more

timely reporting. It is conceivable that some de-emphasis may occur on the traditional problems, and that this will entail a reorienting of scarce skills, i.e., linguists, research, analysts, report writers, etc.

Hour for hour and pound for pound of intercepted traffic, diplomatic communications provide the best yield of economic information, whether the traffic is encrypted or plaintext. It is for this reason that no let-up in the intercept and processing of diplomatic traffic should be considered in order to increase the output of economic SIGINT.

We must, if anything, increase the flexibility of processing and reporting such traffic. The nature of the economic problem will be such that we may be required to organize, process, and/or report in many forms, with timeliness an extremely important factor. Just as tactical support to a military commander must be timely, and attuned to the various phases of the operations,
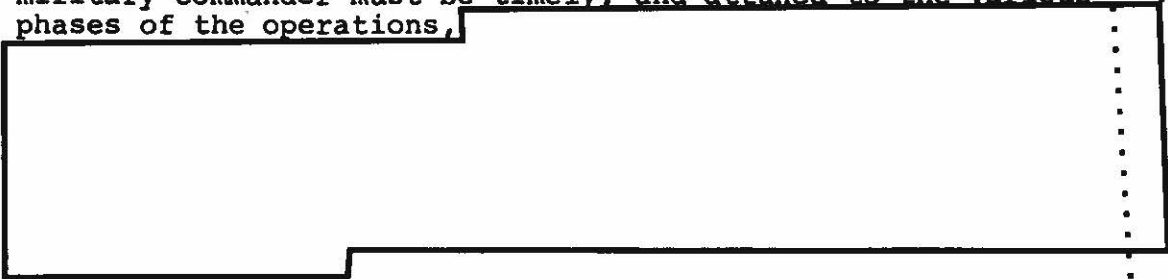
promise to yield mass volumes of such data, which will require mass machine scanning, etc. These processing techniques are currently being tested, and it is hoped that the increase in human effort can be kept to a minimum; however, it would be unrealistic to hope that no increase in linguists, analysts, or report writers will be required for an increased economic effort.

A de-emphasis of traditional military problems because of a relatively relaxed international atmosphere will undoubtedly permit the reassignment of some personnel from these problems to the possibly emphasized economic ones. By no standard can we expect an increase in any resources of NSA in these times of stringent budgets. We must be looking for better machine-processing methods, machine outputs designed to meet customer

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

requirements with the minimum of narrative, information banks
which can be readily queried, etc. Only by the adoption of
these techniques can we ever hope to cope with the increased
volume of material and the possibly increased requirements.

In addition to providing [   ] to the traditional
Departments and Agencies, all of whom have supporting intelli-
gence production organizations, we must consider new members
[   ] organizations that may not have SIGINT analytic
support integral to their organizations. In these instances we
must plan for providing the required support in easily readable
form, devoid of SIGINT jargon and intelligible without recourse
to special interpretation.

> *NOTE: This article appeared in the January*
> *1973 issue of Keyword and is reprinted here*
> *with the kind permission of the Editor of*
> *Keyword and the author.*
>
> *In view of the changing relationship*
> *between the United States and Asian countries,*
> *particularly the Peoples' Republic of China,*
> *one may expect an increased interest in*
> *economic SIGINT from B target areas.*

****

"Shall I tell you what knowledge is? It is to know
both what one knows and what one does not know."

----Confucius

THE GROUND ZERO APPROACH TO LANGUAGE ANALYSIS
by Dan Buckley, B61

The "ground zero" approach to language analysis is the
mechanical application of language skills (at whatever level
of competence) to a particular target on a day-to-day basis,
without regard for anything that happened yesterday and with-
out concern for what may happen tomorrow--or beginning each
day at "ground zero." It's easy, comfortable, and best of all,
it's safe. Like most people, linguists have security blankets.
Among their favorites: "I know what it says--you figure out
what it means." This is closely followed by the nonsensical
replacement of foreign words with English equivalents (more
or less). For example, in Vietnamese this results in
"dropping 200 pounds sterling bombs" for *nem bom 2000 bang
anh* or "active activity" for *hoat dong tich cuc* rather than
"2000 pounders" and "positive action." Does "ground zero"
then become *mat khong?*"

At any rate, the "ground zero" approach is more than safe;
it is irresponsible and ineffective. You can't work traffic
successfully with such a method because you can't know what is
abnormal (reportable) if you don't know what is normal; and you
can't know what is normal if you know only what is happening
today. You have to know about yesterday and care about
tomorrow--and then you have to do something about it. Here
are some things you might try to cure the "ground zero"
syndrome:

1. Constantly improve your language capability. Don't
use cipher traffic to do this unless you never read it as
part of the job. If cipher traffic is your field, read plain-
text for practice. Newspapers are even better because while
reading traffic won't help your vocabulary and structure
problems much, newspapers will; and the newspapers will help
you to read traffic.

2. Have your translations checked occasionally, especially
one that you consider well done. It doesn't do much for the
ego sometimes, but it is an effective learning method. Don't
be embarrassed if it's not as good a translation as you thought--
you really need from three to five years of varied experience
to be a highly qualified translator.

3. Don't be lulled (self-satisfied?) into thinking of yourself as a "hotshot lingy" because of practiced facility with a particular group of traffic. Most VE-100 grads could learn to read and work artillery traffic in a week, so you might want to ensure that you aren't confusing expertise with familiarity. Try not to spend more than a year at the same desk, or rather, with the same group of traffic. You ought to make some effort to expand your qualifications, keeping in mind that undeveloped people tend to make a significant contribution to their own undevelopment.

4. Practice writing out translations in good English. The best translation is one that reads as though it was never in any other language. *Nha cua anh Tam* ought never to come out "the house of Mr. Tam"--why not "Tam's house?"

5. Don't mistranslate anything, ever. Sooner or later you are going to have to come to grips with a fact of the translator's life: there are some things you don't know. Socrates had something to say once about the really smart guy knowing the limitations of his knowledge.

6. Be specifically aware of everything that happens in your traffic and generally aware of what's going on about you. The "lingy" working the traffic is the duty expert--make no mistake about it. If you don't know the little things that happen every day and their relationship to one another, there is probably no one who does know.

7. Keep records. That's the answer to the question generated by paragraph 6. Keep records on OB, personalities, locations, and events at least on a system/unit basis. It helps you to keep track of what's going on, helps with crypt-system identification, and in the event of your untimely departure it helps the next guy get snapped in that much faster.

8. Learn an effective writing style. That really may not require a major change but something as apparently insignificant as switching from passive to active voice: "NVA forces in southern Laos will launch a major offensive..." rather than "It was noted that a major offensive is to be launched by NVA forces in southern Laos..." If you need help here, get it from any of the senior language analysts. Most of them make at least $15,000 a year and you can help them to

earn it. Seriously, every one of them will be glad to help
you, and I can honestly say that I don't know a single man or
woman among them who would feel that you were imposing.

9. Get out of the "bubble." Language is not an end in
itself; it is a tool--nothing more, nothing less. It can be
used in breaking crypt-systems and recovering comms nets, just
as C/A, T/A, and reporting are tools which can help the
linguist. The linguist who operates in the "language bubble"
is almost doomed to mediocrity and a performance at the "ground
zero" level.

Finally, you ought to be asking yourself whether you are
any better as a language analyst than you were last year.
What language contribution have you made to your section/branch
that was not levied upon you by someone else? Are you operating
at somewhere near maximum capacity? Is 100 messages a week
truly the limit of your capability? As resources diminish,
someone else is likely to ask those questions--and they are
legitimate. If "ground zero" is your location, there is no
better time to move than now.

****

ວິດ ມີ ຊູ້ ສວວ ຈວກ ບ້ານ ບ້ານ

ຊູ້ ນຸ່ງ ກະໂປ່ງ ຫວວນ ສັນ ສັນ

ລາວ ພົນ ຫະຫວນ ບໍ່ງ

ຊູ້ ໄດ້ ເຮົา ໄດ້ ເບິ່ງ

ແລະ ດຽວ ນີ້ ເຮົາ ຢູ່ ວຽງຈັນ ຫວວນ
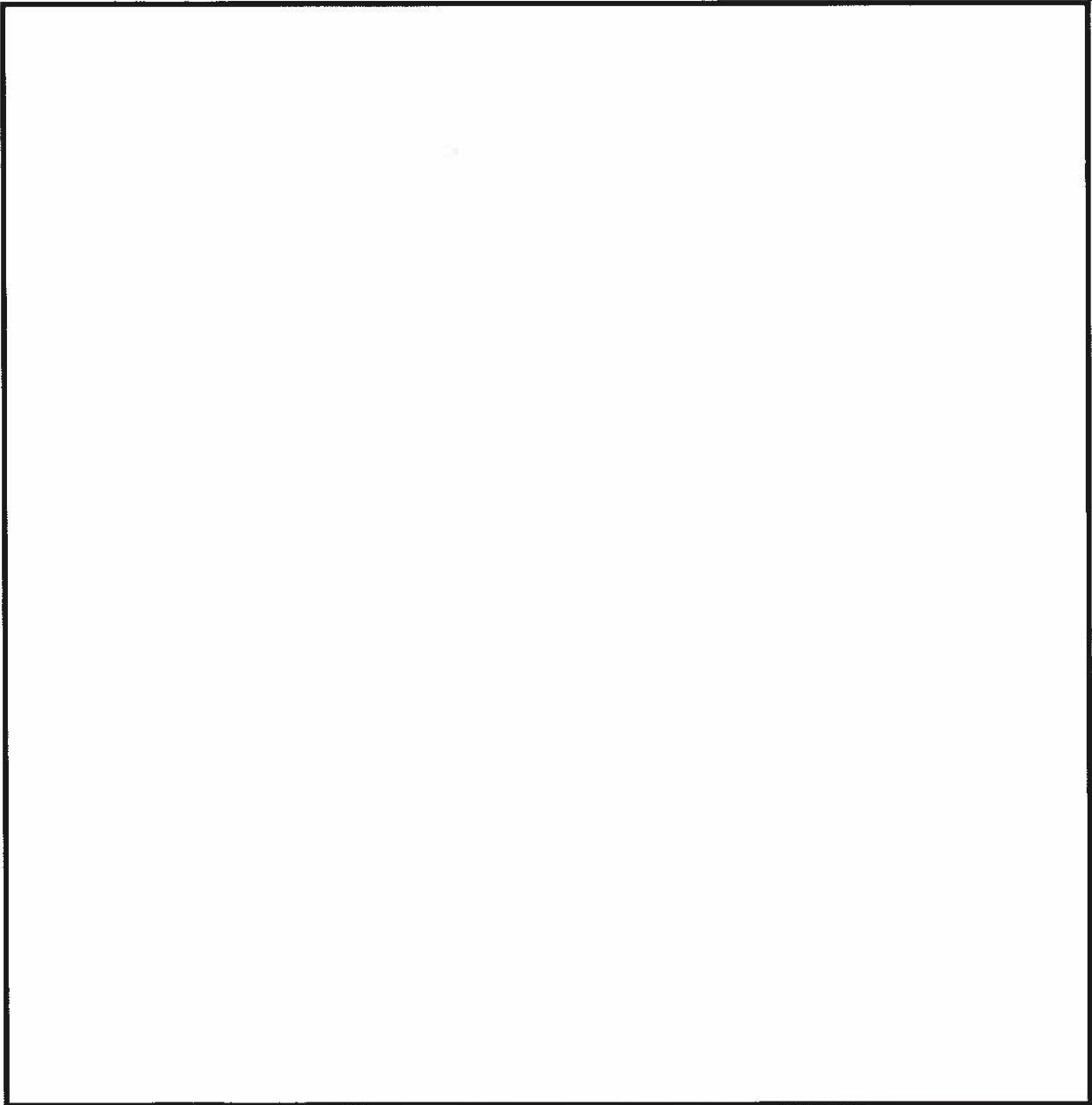
There was a young lady from
     Ban Ban
Who wore her skirts very
     san san.
She met a G.I.

Who gave her the eye

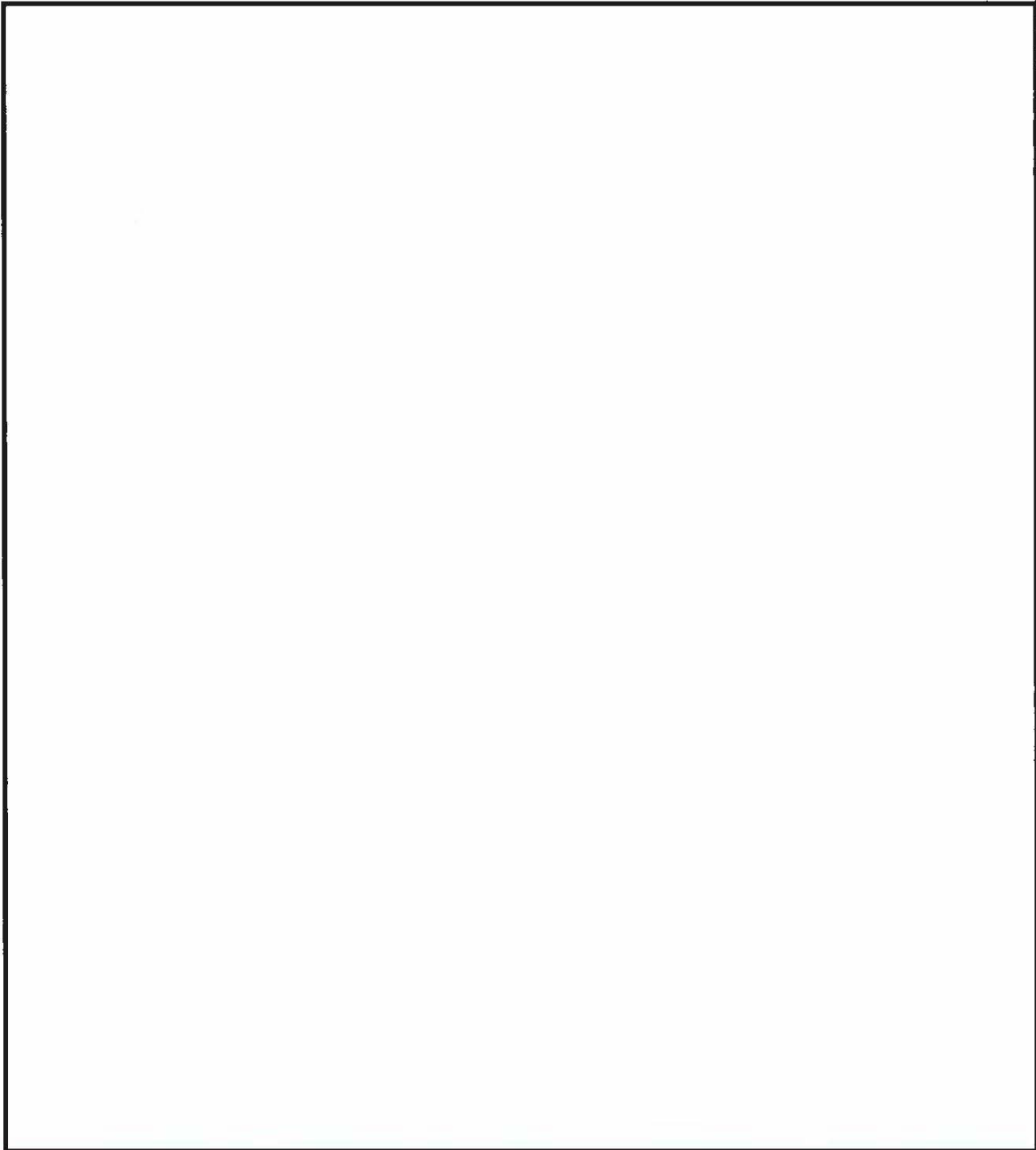And now they live in sweet
     Vientiane.

---Doug Perrit, B12

24

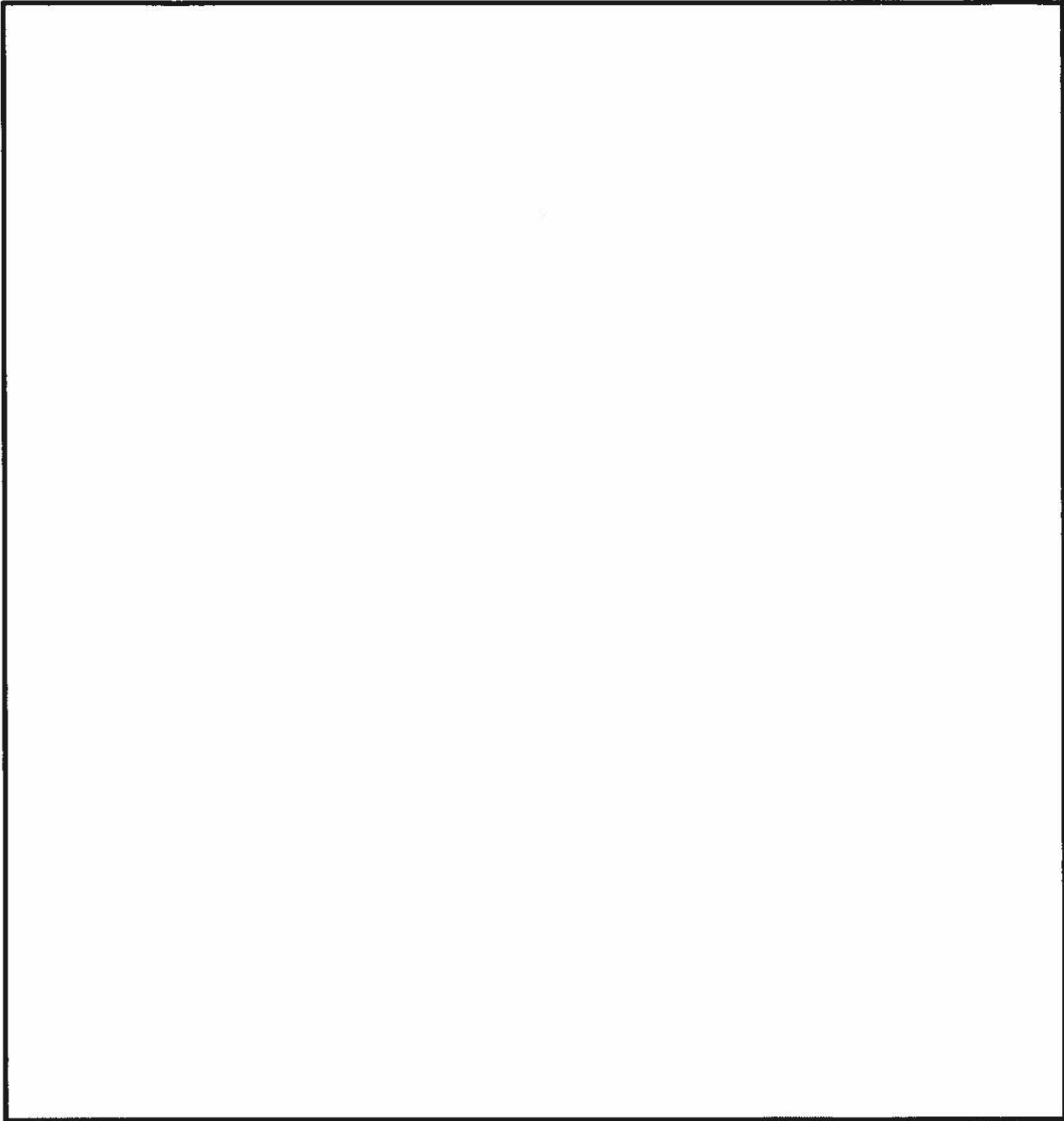EXPLOITING THE BUST
by Kenneth Miller, B43

26

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

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

ONCE MORE THE TSR
                    by Jane Dunn, B45

     The TSR or Technical SIGINT Report is, according to the
pertinent NSA Publication Manual, "a vehicle for authoritative
presentation of significant analytical results which are
sufficiently well established to convey a technical conclusion
or theory and which may be used as a basis for further analysis
and/or product reporting." I believe that this definition
ignores a very important aspect of the TSR--the quality of its
writing.

     We have all heard the pleas for technical reports to
document analysis so that vital technical and historical infor-
mation does not leave the organization with the departing analyst.
High-level concern about deficiencies in our report writing has
resulted in an explosion of NSA writing courses and in the
requirement for evaluation of English competence in the perfor-
mance appraisal of employees above a certain grade level.
Unfortunately, the number of well written technical reports does
not seem to have increased in proportion to the attention given
in recent years to the "English" problem. Although a poor report
is probably better than none (even if the ultimate reader has to
do some textual analysis to discover what the writer is trying
to say), there is little excuse for poor writing in an agency
like ours where the average level of formal education is excep-
tionally high.

     As bad money drives the good out of circulation, so poor
writing overwhelms the excellent and drives it underground. We
become so accustomed to the dreary procession of cliché, jargon,
and stereotype that we risk losing our power of discrimination.
Standards slip lower and lower until what has been described as
"illiterate garbage" becomes the accepted norm, and only the
occasional appearance of a well organized, informative, literate
piece of technical writing reminds us that we can do better.
But how? Perhaps the first step in the steep climb toward
excellence is to take a good look at some of the technical
reports we have ourselves produced or read.

     Rarely does a SIGINT target organization send or receive a
cipher message; encrypted traffic is transmitted by some entity
in communications with another. Nor does any monitor intercept
such a message; encrypted traffic is observed being passed by

subject entities. A Polvetzian regiment seldom uses PQMR-127
for daily strength reports; a PQ regimental level military
entity is presently utilizing cryptosystem PQMR-127 for daily
reporting of personnel strength. In fact, nothing is now used;
it is presently being utilized. Such overblown verbiage is
hard to swallow the first time it appears; when it is repeated
in all appropriate slots in a stereotyped format, it becomes
downright sickening. Is it any wonder such reports pass quickly
across the desk and into the burn bag or the darkest corner of
a file drawer?

From the evidence of published TSR, the prospect of writing
a technical report must terrify many analysts. Faced with
producing such a report, the writer scurries to the files for an
earlier document which he can republish after substituting more
current dates and adding a handful of new details. He thus has
a security blanket, but does he have a report? The published
result is not the product of analysis but the regurgitation of
an analyst's card file. The nadir of technical reporting is to
publish a printout of an IBM deck under a TSR number and title.

Another security blanket for the technical reporter is the
check-off list designed as a memory aid but too often used as
the incorporated outline for a TSR. Relying on such a grocery
list leads to the deadly practice of making some entry under
each heading even if that entry is "Nothing to report" or "Not
applicable." Both the "update" and the check-off list allow the
writer to withdraw, however ungracefully, not only from taking
responsibility for analysis but also, one is tempted to conclude,
from thinking.

Guidelines for effective writing abound. They cover the
field from "correct" grammar and punctuation to hints on writing
style. The analyst who seriously wants to improve his technical
reports will find that he gathers dividends from an investment of
time and, if necessary, money in using such aids. At the very
least, the investor will avoid the danger of having his conclusions
dismissed as unreliable because the reader equates poor writing
with fuzzy thinking.

CRYPTO-SCRAMBLE

Ray Titus

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

1. O X O P I A N T I T L E
   _ O _ _ _ _ O _ _ _ _ _

   Production of information from messages that are encrypted in systems whose basic elements are known.

2. E N P A B S T S O I L O
   O _ O _ _ _ _ _ _ _ O _

   Used to determine causal or random repetitions.

3. N A K K Y B E
   _ O _ _ O _ _

   File of available keys.

4. A R T M E N O T E
   _ _ O _ _ O _ _ _

   Group of 4 digits

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

"I first got the idea...."

Print CRYPTOANSWER here :

Sounds like the confessions of a skyjacker.

— — — — — —   — — — —

Answer on page 37 .
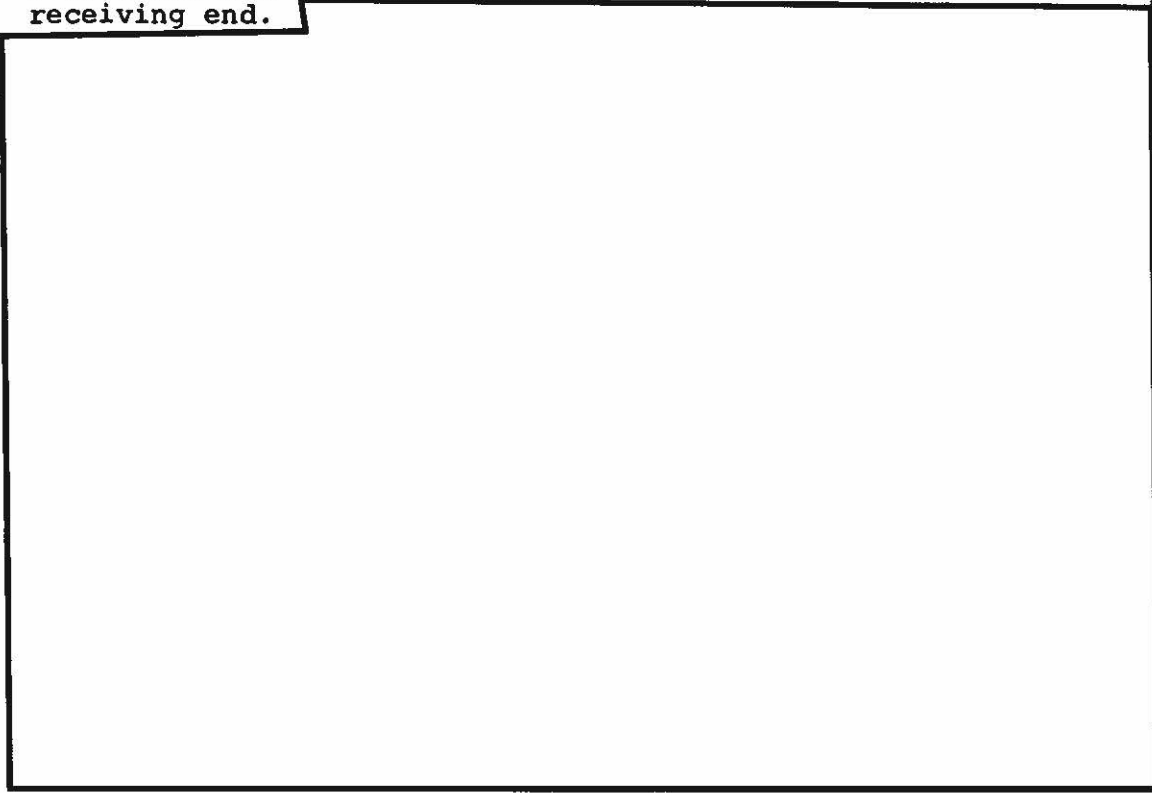
EO 3.3b(3)
PL 86-36/50 USC 3605

HOW ABOUT THE OLDSMOBILE M?
                        by Thomas Wood, B34

     At the start of the "air war," when the bombing of
North Vietnam began in earnest, the neighbors to the north
were concerned <u>that they might become involved---on the</u>
<u>receiving end.</u>

     Having reached the correct solution (albeit incorrectly),
we saw no reason to advise the customer of any anomaly in
the text of the published translation!

STANDARDIZATION????
            by Russ Myers, B12

        Three data preparation media to ready messages for insertion
into the FASTRAND drum file are available to bookbreakers using
Project TREES on RYE. They may punch the messages onto ASR-35
paper tape in *ASCII* 7-level coding or onto cards via the IBM 029
keypunch in *EBCDIC* coding or the IBM 026 key punch in *FORTRAN-H*
coding. The ASR-35 handles   the translation of *ASCII*-coded
paper tape into internal   RYE *FIELDATA* coding; however,
a "translation" card   must be provided with card
input. If you are using   a SORBAN card reader,
without its own   internal coding, you
need only provide   for translation from
EBCDIC card code   or *FORTRAN-H* card code
to RYE internal   *FIELDATA* code, as approrpi-
ate. However,   if you use a UNIVAC-1004
outstation, the   "translation" card will
facilitate the   conversion from the
UNIVAC-1004 oriented   *XS-3* coding to *FIELDATA*
coding. The Project   TREES program, OLIVE, will
conveniently copy a   RYE FASTRAND message file
onto magnetic tape.   The tape will be *BCD*
coded. I suspect some-   thing was lost in
"translation" when my   sponsor did not recognize
the special characters on the message file tape I provided him
when he listed it on his Burroughs B300 outstation in *BCL* coding.

* * *

----OR CONFUSION????

SEEDLINGS
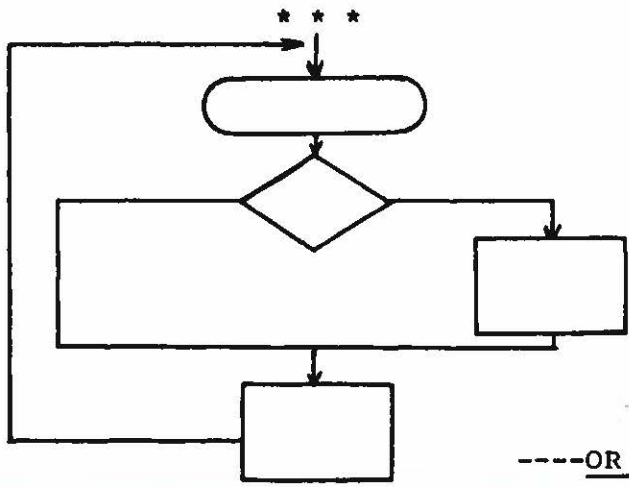
----B GROUP EXPANDS; NEW OFFICE ESTABLISHED. The Office of Asian Systems Development, B7, with Mr. Coleman Goldberg as chief, came into being 8 February 1973. This new addition to B Group will be responsible for initiating, coordinating, and implementing a comprehensive program for upgrading the PRC collection posture and improving the management of B collection assets.

****

----The revisions in the criteria for professionalization in several career fields are highlighted below for your information. If there are any questions, please contact your training coordinator or the Executive of the individual panels.

·Special Research: A written Professionalization Qualification Examination was instituted as of 15 January 1973. The oral interview will still be required if an aspirant scores between 70 and 80 on the PQE or at the option of the Panel if a score of 81 or above is obtained.

·Traffic Analysis: Effective 1 January 1973, the basic requirements for certification in the Traffic Analysis career field are 1) high school graduation or certificate of equivalency; 2) a documentary report acceptable to the Panel; and 3) passing the T/A PQE which, beginning calendar year 1973, will be offered only once a year. This year, Part I will be offered in May and Part II in December.

·Signals Analysis: The revised criteria, published on 26 October 1972, differs in two ways from the old. The first is that maximum performance points have been dropped from 500 to 250 points; the minimum remains at 150 points. To obtain points in this category, a candidate must submit a technical or methodical report which presents either a signals processing or analytic approach or system conceived by the candidate, the results of such an approach or system, or the results of a signals or telemetry analysis effort. The second difference is that computer and physical science courses have been added to the list of related courses.

--By the way--the Cryptanalysis, Language, and Traffic Analysis Career Panels have been relocated to 3C051.

****

34

----Did U Know? There is a "Hot Line" in the main NSA Building. YES--a 24-hour recording device is in operation in the office of the Senior Enlisted Advisor to the Director, NSA. The purpose of this "Hot Line" is to make available a round-the-clock method of helping the enlisted personnel stationed at NSA with any problems that cannot be resolved through normal channels. To use this outstanding service, just dial "IDEA" (4332s).

****

----L14, the Transportation Office, has been conducting a series of surveys about establishing commuter bus services in various areas such as Columbia, Md., and Washington, D.C. Personnel willing to support those services or interested in initiating other services should contact the Transportation Officer, L14.

****

----Congratulations to Virginia Valaki and her cohorts in G5 for successfully penetrating an

****

----BLITZ COURSE ON RYE...The Cryptanalysis Department of the NCSch is offering a new course, called RYE Operations for Cryptanalytic Applications. CA-090 is designed to give the working cryptanalyst practical experience in using RYE effectively as an aid in solving cryptanalytic problems. The course length is two weeks, half-time. It includes detailed discussion and usage of 15 GUPPY programs. Prospective students should have a working knowledge of cryptanalytic terms and techniques (CA-100 level). The first class is being offered in March. For further information, contact the CA Department, 8025.

****

----On 23 January 1973, the Language Career Panel held its first formal graduation ceremony in the Director's Conference Room, at which time 23 language interns, representing eight languages, received letters of completion of the intern program. Thirteen of the graduates also received Professional Linguist certificates.
   Mr. Robert K. Hess, Chairman of the Language Career Panel, opened the ceremony with a capsule report of the Language Intern Program. He then introduced the Language Career Panel Members, Advisors, and Staff, former Executives, and

~~TOP SECRET UMBRA~~

Language Intern Sponsors. Dr. Louis W. Tordella, Deputy Director, addressed the graduates on the subject of language work at NSA. He was assisted by Mr. John J. Connelly, ADPM, in presenting the certificates ·to the graduates.

The ceremony was followed by a brief reception· which featured sparkling punch and petit fours.

The graduates and the languages they represent are:

*Daniel J. Allman, Japanese
[   ] German
 Carol Buschbaum, French
 David G. Chizum, Russian
 Donald H. Deitrick, Korean
*David G. Dillard, Spanish/
                   Portuguese
 Gerald L. Everett, Spanish
*Linda L. Franklin, French
*Richard L. Gibson, French
*Marjorie D. Hamlett, Spanish
 Margaret K. Keirstead, Spanish
 Terry L. Lyons, German
*Carole A. McGee, Arabic
*William S. Olmsted, Russian
 Veronica J. Palk, Arabic
*Michael G. Pond, Russian
*Martin J. Savalchak, Russian
 Sheila B. Singer, Portuguese/
                    Spanish
*Susan L. Smith, Arabic
 Arlene M. Sullivan, Japanese
*Joanne L. Urban, Spanish
 Florence E. Wagner, Shan
*Georgianne M. Weiser, Arabic

*Graduated with Certification

****

----Would you believe that G8 didn't find out until 27 February that B1 had relocated to FANX II from FANX III in October? There just ought to be a law!

****

----Papers for The CLA essay contest can be submitted through 31 March 1973. Send three copies to Mr. C. G. Pritchard, Secretary CLA, B5111, FANX III. Prizes of $100, $50, and $25 will be awarded at the Annual Banquet (date to be announced). The criteria for judging the contest are:

   a. Relevance to the cryptology of the subject and treatment.
   b. Interest of the paper to NSA professionals.
   c. Style of writing.

For security rules, consult the Technical Journal, Vol XI, No. 4, 1966. Papers that you have written concerning your regular assignment may very well be candidates for submission.

Don't forget the deadline date-- 31 March.

****

----Keep 7 and 8 May open dates on your calendar. That's when the Institute for Advanced Technology (Control Data Corporation) is holding its seminar on Data Base Concepts in the Washington, D.C.

~~TOP SECRET UMBRA~~

area. This seminar will provide management with a general understanding of data base concepts. In particular, management's role in the design and implementation of the data base will be addressed.

Other dates of interest are 25 to 27 April, when the same sponsor will hold its local seminar on Advanced Programming Techniques. The seminar, designed for programmers, analysts, and their technically oriented supervisors, will deal with philosophies and advanced techniques of computer programming. Ideas applicable to any machine and any programming language will be discussed. Special attention will be given to FORTRAN, COBOL, PL/1 and assembly languages.

****

----The joint meeting of all members, past and present, of the TA, CA, LA, and SRA Intern Programs scheduled for 14 March in the NSA auditorium will be reviewed in the next issue. The guest speaker will be Mr. David Y. McManis, Chief of the White House Situation Room.

****

----Smiles and Tears: We are happy to announce the recovery of two members of the *Dragon Seeds* staff: Ray Lynch, B44, from a heart attack, and Lorna Selby, B1, from an eye operation.

Victor Tanner, our Rewrite Editor, has turned in his red

pencil and is off again to Vietnam (his fourth or fifth tour). [   ] formerly of the Press Corps, is enroute to the same destination.

****

Solution to puzzle:

1. Exploitation
2. Poisson Table
3. Key Bank
4. Tetranome

Crypto-answer:

Plain Text

****

TUNNEL VISION

----As glaucoma can lead to total blindness, ignorance of other disciplines can lead to total analytic failure. The cryptanalyst who ignores station identification and traffic laning deprives himself of a most valuable tool and can insure smearing of any statistical values which could give the system away. The traffic analyst who ignores crypt discriminants and indicators similarly throws away clues to station ident and callsign system structure and usage.
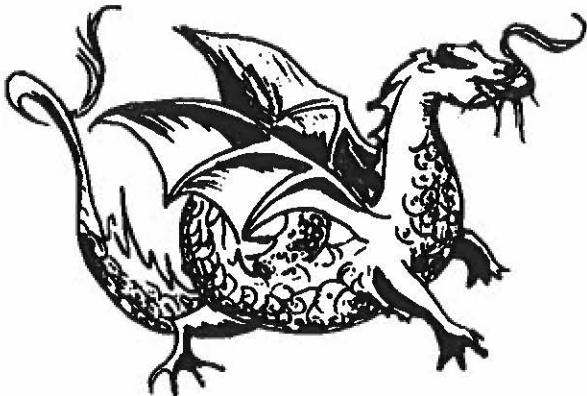
ASK

THE

DRAGON

LADY

TO: Mr. Leon F. O'Meara, C5

Dear Mr. O'Meara:

The following questions were submitted to the Dragon Lady by B Group open-shop programmers. We are forwarding them to you with the hope that you and your staff of experts will enhance our enlightenment by supplying the answers.

1. For any programming application, the maximum result is attained by a Time Sharing Option (TSO). The programmer sits down, programs, debugs, and executes in what appears to be an on-line one-on-one environment. Time Sharing Systems are used to service many programmers at different locations. The RYE System is the closest thing NSA offers to a TSO. APL is a real TS system but, because of restrictive file capacity and lack of resources, is not a practical alternative. The question, then, is: With all the resources--CPUs, ASRs, 2260s, and APL terminals--and a large debug workload, isn't it time for such a service to be made available to open-shop programmers?

2. "Re-inventing the wheel" is a cute phrase around NSA, and also a daily occurrence in the programming field. Why isn't there a readily available multi-volume set of program, machine, and system descriptions representing a central repository of information? Why isn't there an updating service for technical manuals which incorporates additions and explanations by the technical staff to further the dissemination of information?

3.   There is more than enough work to go around.
With that as a basic premise, wouldn't it be better to
permit the programming staff to attack any problem in the
language which suits it best, rather than introducing new
languages of dubious value? Also, wouldn't it be logical to
standardize languages across several machines (i.e., FORTRAN,
IBM 370H, B6700, RYE, etc.)?

4.   How is change effected? Is a more responsive
mechanism than the Suggestion Program needed in the area of
data processing? Are we afflicted with the "not-made-here"
syndrome?

You can appreciate our reluctance to tackle these queries
and can understand our urgent request for assistance. We
would like to include both the questions and any rejoinders you
may supply in our next issue.

DRAGON LADY, B03

Dear Dragon Lady:

I hope that the following will be adequate answers for
your questions. Further clarification can be obtained from
appropriate C5 representatives.

1.   IBM defines time sharing as "the shared, conver-
sational, and concurrent use of a computing system by a number
of users at remote terminals." TSO (IBM's Time Sharing Option)
is designed, according to available documentation, to provide a
time sharing environment for terminal-oriented applications.
It provides the user at a terminal with a command language with
which he can develop, test, and execute programs conveniently;
it also contains data entry, editing, and retrieval features.
Time sharing jobs entered from the terminal (foreground jobs)
share system resources with batch jobs (background jobs) that
are being processed at the same time.

TSO appears to have numerous advantages for programmers
and users in a terminal environment. However, there are several
restrictions involving its use which must be studied. No single
software package is the answer to everyone's prayers; TSO's
apparent benefits are not without balancing drawbacks. Some OS

facilities are unavailable to foreground jobs; the execution of
all jobs may be seriously affected if TSO is not appropriately
"tuned" for our regular job mix; the monitoring of system use
and performance becomes a highly complex job; and security
problems--the needs for adequate data and program protection--
are increased.

C Group is hoping to obtain, in early Spring 1973, an IBM
370/155. One of its principal uses will be the test and evalua-
tion of TSO for use at NSA. We hope that by careful study and
experimentation with different facets of TSO we will be better
prepared to calculate its effects on our overall data processing
efforts. We can then fit TSO into our systems with a minimum of
upheaval and discomfort for users.

2. We agree that a great need exists for a central
"library" of data processing information. Most offices in
C Group maintain their own libraries in a more or less haphazard
manner. The P2 Technical Library maintains several shelves of
technical information concerning computer hardware and is an
excellent source of generalized information on "what's available"
in the marketplace.

Within C, C5 and C9 are attempting to create a computerized
facility containing information about our own hardware systems.
Hopefully, it will contain current information about the resources
of a particular system, the locations and types of terminals, and
the like. The problem becomes an obvious one, however, whenever
the word "current" is used. Some decision must be made about who
will be responsible for updating the file and how information
will be filtered to that individual or organization whenever
changes are required. It is not a simple matter.

Technical manuals are a different kind of problem. C9
attempts to make available the latest updates to IBM and Burrough's
manuals. Information is supplemented by "User Bulletins" published
by the C9 offices responsible for the various systems. C7 also
publishes "Technical Bulletins" designed to make users aware of
any changes which might affect them. Beyond this, C Group does
not, at the present time, have the human resources to cope with
a problem which is, admittedly, staggering.

3. We believe that for any given programming application there are a variety of factors which should be considered in determining a preferred computer solution. Primary factors include the following:

(1) Accessibility of the data file(s) as input to the program on the preferred computer.

(2) Adequacy of the computer resources for the demands of the application.

(3) The needed type of user access to the computer environment.

(4) The programming language and associated compiler which best meet the demands of the application.

(5) Availability of the preferred computer resource for the specific application.

(6) Priority of the application in relation to other demands for the preferred computer resource.

Secondary factors which might affect the computer solution include the following:

(1) The availability of a programmer.

(2) The programming language repertoire of the available programmer.

(3) The presence of a computer which is not as heavily loaded as other choices.

A program for a manager of programmers is to minimize the impact of the secondary factors, particularly if they force an undesirable compromise on the primary factors.

To be more specific on the first part of Question 3, we believe that selecting the best programming language for a given application is a very important process and should be done in light of the above factors. C has a software division (C95, the Languages and Compilers Division) whose services are available to assist the user in this process. In addition, this division provides direct customer support for solving problems

in using a programming language or its associated compiler. A
telephone call to secure extension 4745 will tap this service.
We also believe that a programmer with a working knowledge of
several programming languages and compilers can do a better job
in matching an application with a language than he can if he
relies solely on one or two personally favorite compilers.
Further, we think it is desirable for the open-shop programming
manager to know which languages and compilers are supported by
C Group and, equally as important, to know why each one is
selected for support.

Briefly, C supports those programming languages and
compilers which can provide the best production service to
the NSA community. More specifically, C95 currently supplies
nine higher-level programming languages and 23 associated
compilers on our general purpose computers. All of these are
proven, production grade resources. C95 is available to provide
information for parties interested in specifics. To our know-
ledge, we do not "introduce new languages of dubious value."
C9 employs a careful and critical review process before intro-
ducing a new language or a new compiler to the user community
for production purposes. Part of this review process is to seek
and consider the views and requirements of the user community.

To address the second part of your Question 3, an analysis
of FORTRAN on the family of NSA computers was performed in 1967/68
with the objective of standardizing across the board. We
discovered that the task would have been formidable for two
primary reasons:

   (1) As a language, FORTRAN is not rich enough
to assure compatible meaning on different kinds of computers.

   (2) No two of the FORTRAN compilers used at NSA
are built with the same compiler technology.

Further elaboration can be found in an article, *Program Trans-
ferability*, in the *Proceedings of the NSA Network of Computers
Conference, 1968 (NOC-68)*. A more recently published report
titled *C95 Technical Bulletin No. 35, FORTRAN COMPARISON*, March
1972, is also available. To respond to the need for a standard
programming language, we are building the NSA BETA language and
compilers that are designed not only to avoid the above FORTRAN
problems, but also to provide an algorithmic capability well suited
to the needs of the open-shop cryptologic programmer.

4. The problems of effecting change vary according to the size and complexity of the applications software system involved. If the software is a single purpose application system of moderate size, speed of change is mostly dependent on the availability of manpower to make the change. If, however, the software system involved is a large general purpose system such as KAY or GENED, there are often extremely difficult technical problems in either modifying or adding to the system. For example, one of the GENED problems which beset us for many months was the limit on the size of the error file. When the allowable file size was exceeded (an altogether too frequent occurrence), the system could not process any more data. A program change to expand the error file size seemed to be a simple solution, but detailed investigation by the software specialists who knew the system best showed that this seemingly simple change had cascading effects which would have necessitated a complete rewrite of the system. This investigation, in addition to studies of alternate solution, took weeks to accomplish. There was no "not invented here" syndrome in this problem; it was simply a very difficult technical problem that took a long time to resolve.

This example is indicative of the difficulties of making apparently simple changes to a complex system. There are, I am sure, examples of desirable changes to comparatively simple systems not being made because of the NIH syndrome. The best way to resolve this type of situation is for the line manager in the analytic area to discuss the proposals with the line manager (at Division level) in C5. A valid requirement or a worthwhile proposal should not be allowed to die at the analyst-analyst level. Managerial review is essential in these cases.

* * *

The Dragon Lady offers her humble apologies to Piqued, whose question in the December issue was unanswered...a composition error. In correction, she submits the following.

Many people have asked "Why the TACP does not accept applicants for the T/A Intern Program if they have had more than two years cryptologic experience?" The selection criteria referring to experience states, "Must ordinarily have at least one year of T/A experience at minimum GGD-07 or E-5 level; however, must

not have more than two years of cryptologic experience at GGD-07/9 levels." (See O/M Subject: NSA Intern Program Vacancies, dated 28 August 1972.) I asked the Executive of the T/A Career Panel to comment on this. His views are:

"When people apply for the On-Board T/A Intern Program they are asked to submit a complete PQR with the other necessary forms. These PQRs are evaluated against the T/A Criteria for Professionalization. The general rule of thumb applied is that applicants with more than 600 points are considered well on the way toward the certification goal of 1000 points and certification. The accumulation of points over 600 is generally due to the experience factor or more than two years T/A experience as a GGD-07 or E-5.

"This is not, however, a hard and fast rule, since the TACP did accept an individual in the past for the program with more than two years T/A experience at the GGD-07 and 9 levels and an accumulation of over 700 points. The plan in this case was to arrange for an abbreviated program for this man. I say *was*, because he was also selected for an overseas position and chose to take that assignment in lieu of the T/A Intern Program.

"To sum up--each case is evaluated on its own merits. The Panel considers whether or not the applicant shows professional potential and weighs that against what the T/A Intern Program offers. The Panel is guided by the need to fill professional level positions in P; and in the selection process of on-board interns, the Panel tries to pick the best. Other selection criteria are listed in the announcement mentioned above."

* * *

If you are standing upright, don't worry if your shadow is crooked.

----Fortune Cookie

CONTRIBUTORS

DAN BUCKLEY first came to work at NSA as a Marine in 1963
     after driving by the building 117 times thinking it
     was a shoe factory. He was a language analyst and
     language section chief from 1963 to 1966, except when
     he was on TDY to Da Nang or Khe Sanh or Phu Bai or Chu
     Lai. He solved the Vietnam TDY problem in April 1966 by
     going PCS to Phu Bai, where he stayed until April 1967.
     On the way back to NSA, he stopped off at Fort Devens
     long enough to finish first in a traffic analysis
     course of 44 students. In October 1970, he left the
     Marine Corps and came to work as a civilian for the
     Agency. He was certified by the language panel in
     March 1969 and by the SRA panel in February 1972. He
     is currently serving in an overseas billet in Southeast
     Asia.

RICHARD CHUN is Chief of the language Support Branch, B443, a
     newly established organization which provides a centralized
     Chinese voice transcription and translation service for B
     operating elements. Mr. Chun joined NSA as a civilian in
     August 1962 after having served in the U.S. Army for 21
     years. His introduction to cryptologic activities came when
     he was assigned to Headquarters, ASAPAC, as the first
     Korean linguist in the field. In June 1953, he headed the
     ██████████ problem at NSA and a year later, was assigned
     to ASA units in Korea and Japan, where he worked on ██████
     ██████████████ problems until spring of 1967. His
     subsequent assignments include Deputy Chief of B27 (B11),
     Chief of JSPC-34 ██████████ Deputy Chief of B34, and Deputy
     Chief of B44, in that order.

JANE E. (BETTY) DUNN's connection with SIGINT dates back to
     WWII and covers targets from Japanese Military to CHICOM
     ██████████████ with stops along the way for work on ████████
     ██████ European Satellite, and Vietnamese Communist
     cryptosystems. She holds a B.E. from Duquesne University
     and was prepared to teach French in Pennsylvania high
     schools before she was detoured to Arlington Hall. Betty
     is a certified cryptanalyst, a tutor for the CA Intern
     program, an E.E.O. counsellor, and the biographic editor
     for Dragon Seeds. Since May 1972, she has been Chief of
     B45, the PRC ██████████████████ Division.

WILLIAM G. FLYNN, B605, has been with NSA and predecessor agencies since 1952. Most of his more than 20 years cryptologic service has been spent within B Group, with limited assignments with P and D elements. A certified Special Research Analyst, he is currently assigned to the Intelligence Staff for all Communist Ground Forces activity in Southeast Asia. He has spent the past five years as the Special Project Officer for B6, and one of his projects was his involvement in the events of the Butcher Case.

WILLIAM HUNT is a graduate of the Marconi Radio Officer's School and completed a one-year college course in the Russian language. He has been continuously employed in crypto-logic activities in the U.S. and overseas since 1940, serving in NSA and other cryptologic organizations in the signals collection, TA, and SRA professional fields. He is currently Chairman of the Signals Collection Career Panel. Among his varied line and staff assignments in NSA Production and staff assignments at the Agency level, Mr. Hunt was the editor of the NSA Daily SIGINT Summary. He is currently serving as a Special Assistant to the Chief, G, developing and coordinating SIGINT Economic Production Plans and Procedures.

KEN MILLER, cryptanalysis technician in B4331, has been with NSA since 1965, with time out for a tour with the Marines 1966-1969. During his first Agency assignment, he worked in B41 on the PRC callsign problem and then moved on to B432, the Research Branch of the Cryptologic Research Division. Here he has spent several years on the PRC high-grade Military [   ] problems, to which he has recently added the Democratic Peoples Republic of Korea[   ]

RUSS MYERS, B1203, joined the Agency in 1965 after serving four years with the USAFSS. Fifteen months of his Air Force tour were spent [   ] one of the "garden spots of the world." At NSA, he spent two years in A8 as a traffic analyst and Russian linguist and then was selected for Class 10 of CY100. He moved to B1203 in 1968 as a cryptanalyst. Mr. Myers was a member of Class 24 of CA-400 and was detailed for six months to B42 under the B Internal Data Systems Training Program. He holds

professional certification in traffic analysis, crypt-analysis, and computer systems analysis, as well as a BA in Government and Politics from the University of Maryland. Mr. Myers is currently involved in the development and management of several data processing projects for B12 problem areas.

GEOFFREY C. WOOD, Chief of B122, came to NSA in 1955 after a number of years in the Navy, serving in submarines and in the Amphibious Force. He was assigned in various capacities to the old ACOM organization, had a tour in the NSASCC, and represented B Group in the National Indications Center. He is professionalized as a Special Research Analyst and is treasurer of the Crypto-Linguistic Association.

THOM WOOD of B341 began his career as a Chinese linguist in 1958 when he volunteered to study the language, hoping for a shot at Monterey so he could stay close to his happy hunting grounds (Santa Cruz) and the lady he happily hunted (the current Mrs. Wood). After completing his language training--at New Haven--he came to the CHICOM [ ] shop, where he demonstrated his immense potential by taking three months to make a single code recovery (DS). For the remainder of his short military career, Mr. Wood was a jack of all trades: intercept operator, "grass" translator, DF operator, and cryppie. Mr. Wood converted to civilian status in the field of his demonstrated potential--cryptolinguistics--and there he has remained. He is a professional linguist who has served and collected souvenirs in [ ] (a bottle of Plum), [ ] (the phrase "show me the way to go home"), and [ ] (Diana and Geoffrey--his two favorite [ ]).

****

STOP !

IT'S

CLASSIFIED ! ! !