~~TOP SECRET~~

National Security Agency

Fort George G. Meade, Maryland

DECEMBER 1972

DRAGON SEEDS

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

Declassified and Approved for Release by NSA on 10-06-2020 pursuant to E.O. 13526; MDR 107694

This is *Dragon Seeds*.

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

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

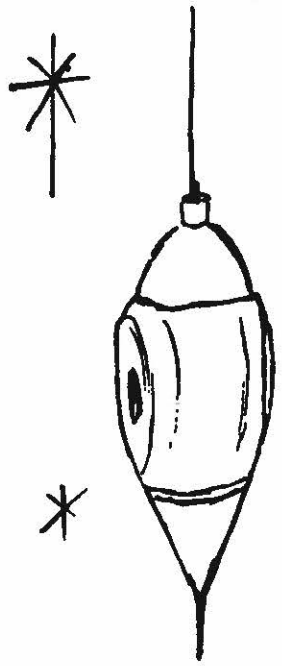
Above all, *Dragon Seeds* is promise. It is fertile with ideas unbounded, to be cultivated with creativity and imagination. It is challenge. It is alive. It will be more than it is.

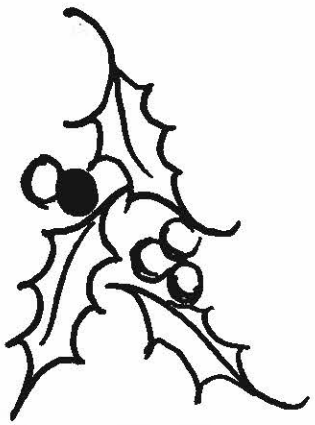
Dragon Seeds is yours. May it grow with you.

The Editors

~~TOP SECRET UMBRA~~

聖誕快樂 新年快樂





~~TOP SECRET UMBRA~~

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

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

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

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

Happy Birthday, Dragon Seeds, and full steam ahead!

H. E. Foslin

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

~~TOP SECRET UMBRA~~

Memorandum

TO : Captain Joslin, Chief B DATE: 30 August 19

FROM : ADP

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

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

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

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

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

Attachment:
a/s

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

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

4 August 1972

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

Dear Admiral Gaylor,

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

Sincerely,

William E. Potts

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

~~TOP SECRET UMBRA~~

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

Helen Ferrone
Lorna Selby

PRESS CORPS

B11 Carolyn Y. Brown	B42 Peggy Barnhill
B12 Philip J. Gallagher	B43 Mary Ann Laslo
B2 Dee Ensey	B44 Jack L. Thomas
B31 Jack Spencer	B45 John E. Uzarek
B32 Jean Gilligan	B5 Nancy Fournier
B33 Louis Ambrosia	B62 [redacted]
B34 Thomas L. Wood	B63 George S. Patterson
B41 James W. Schmidt	B63 William Eley

~~TOP SECRET UMBRA~~

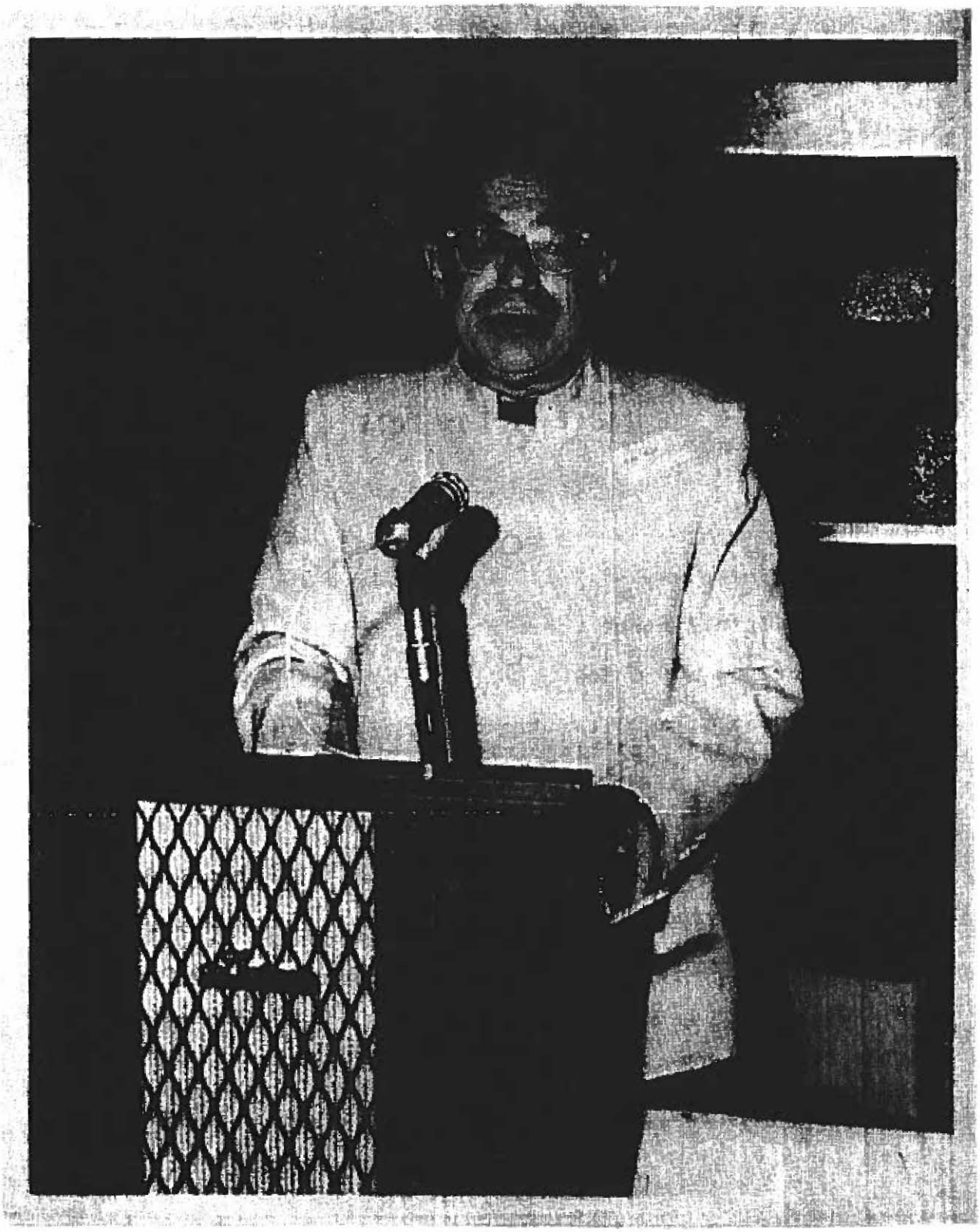
Vol. 1
Nr. V

DECEMBER 1972

TABLE OF CONTENTS

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

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

THE MX-14: A VARIABLE INTEGRATOR

A succinct explanation by Lambros D. Callimahos

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

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

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

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

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

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

CALLIMAHOS...
by Jean F. Gilligan, B32

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

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

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

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

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

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

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

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

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

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

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

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

****

UNCERTAIN ORIGINS

by Tom Glenn, B6

In October 1967 I was the only American civilian within miles of the military complex at Pleiku, Vietnam. I had just arrived on TDY to work with analysts of the 330th Radio Research Company (USM-604). The unit had been there more than a year. It was ostensibly a mobile outfit and was expected to be able to move on command. It had sat in vans, tents, and temporary buildings through the winter blasts of red dust and the summer onslaughts of red mud waiting for a command that never came. It clungwithout roots to its allotted slope on Engineer Hill, all sand bags, watch towers, outhouses and barbed wire, listening intently to the Vietnamese Communist transmitters all around it. Only a civilian, I thought to myself, could really appreciate the profound desolation of a military SIGINT unit mired in Vietnam's western highlands.

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

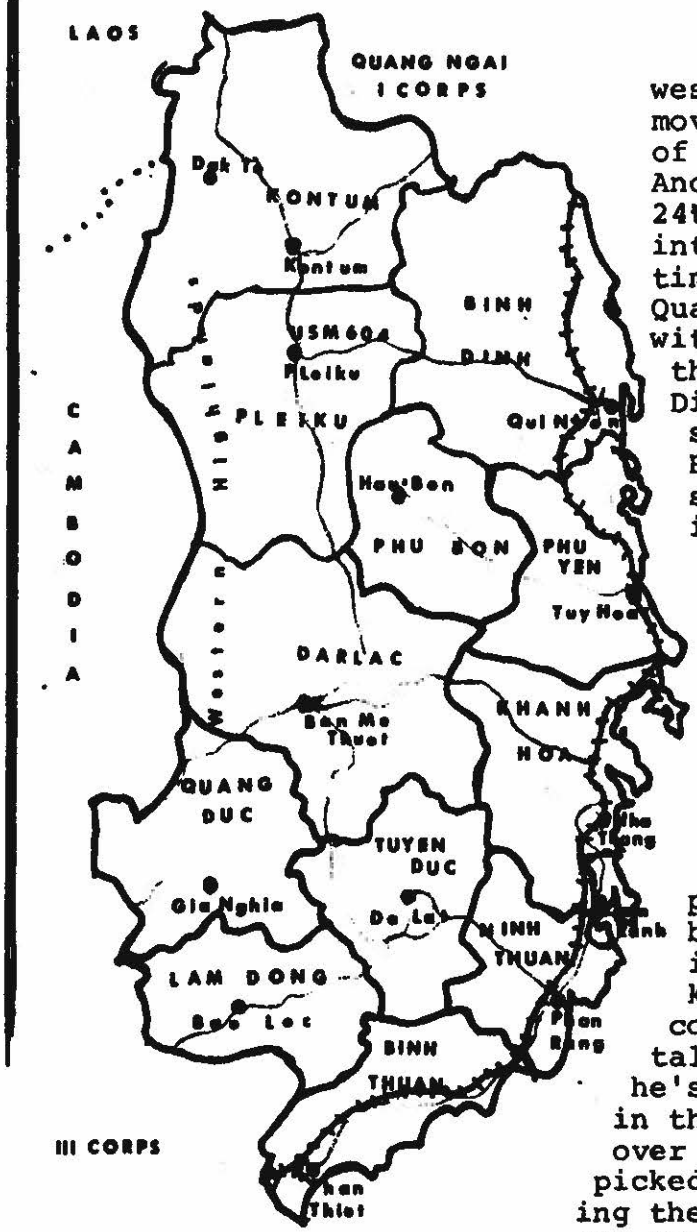
The analysts and intercept operators to a man worked as if their lives depended on it. Most stayed at it twelve to fourteen hours a day, seven days a week, working against colossal odds. The target defied exploitation. Less than one percent of the traffic was readable, the signal plans consisted mostly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

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

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

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

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



NVA B3 FRONT AREA:
Kontum, Pleiku, and Darlac

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

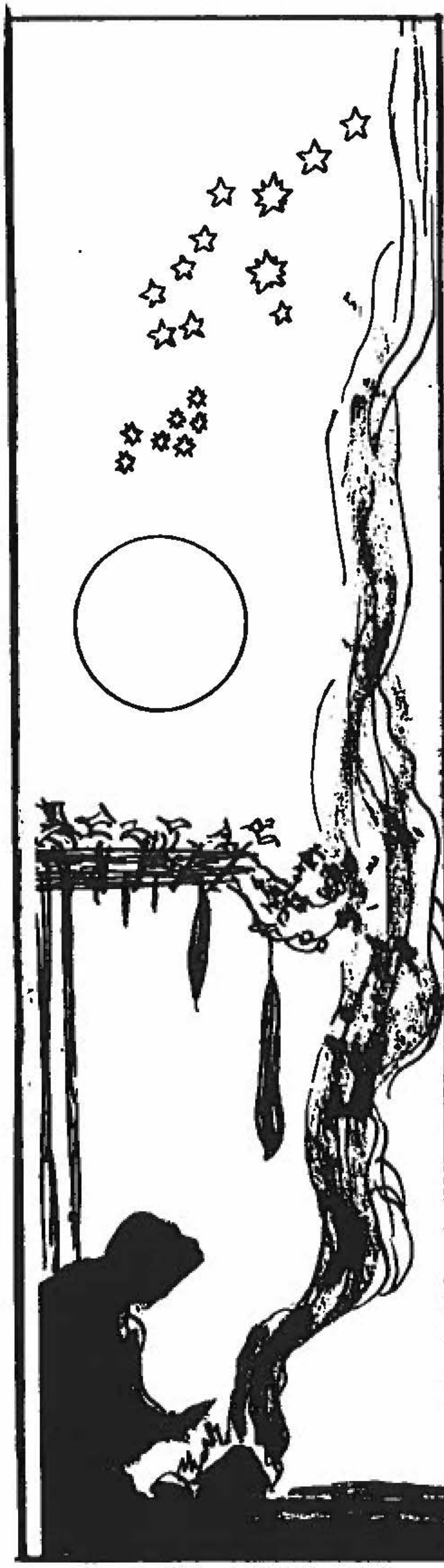
Despite--or perhaps because of--the grimness of what was happening at Dak To, the strain of the increased volume of intercept, and the rising importance, speed, and number of reports and translations, the men of the 330th continued to refine their sensitivity to the ridiculous. Pop Warner was named chief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

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

****

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

****



တန်ဆောင်မုန်းလဖွဲ့

ငွေစန်းရယ်တဲ့ပုဏ္ဏမီ၊
ရွှေကျိုးညိုတာရာနဲ့၊ ကြတ္တိကာယှဉ်ပြိုင်လျှမ်းတယ်၊ ချမ်းစရာသီ။

လှူကထိန် ခါတော်ပွဲနဲ့၊ ခဝဲပွင့် ဝါစိစိ
သာကြည်လို့မြှရှင်း။

လ-တန်ဆောင်မှာ၊ ကြွေပြောင်ပြောင် အသရေ
တင့်ပါသို့၊ ရွှေမြင့်မိုရ်ဝါထိန်ထိန်နဲ့၊
ခါအချိန်မြောက်လေသွေးတယ်၊ နှင်းတဲ့ငွေနှင်း။

ဦးပုံးချို

The Month of Tazaungmon

By U Pyone Cho

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

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

Tazaungmon = November.

Kartikka = A lunar asterism.

Ahlus = Religious offerings.

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

Translated by Kenneth Ba Sein.

THE CINCPAC INTELLIGENCE COORDINATION GROUP -
AN INTELLIGENCE MANAGEMENT CONCEPT

by Walter D. Abbott, Jr., B614

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

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

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

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

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

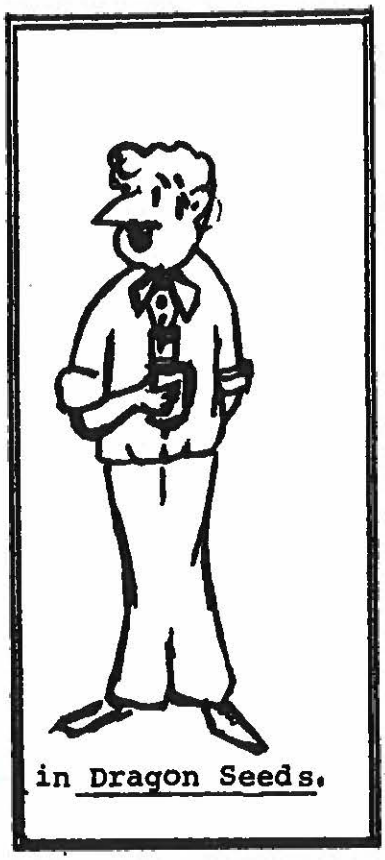
This exploitation of GDRS communications generated several immediate problems for user and producer alike. Based on the number of personnel reported in these messages as heading south, it became painfully apparent that the accepted MACV infiltration estimates were extremely conservative and did not reflect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

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

Happiness is an article ...

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

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



in Dragon Seeds.

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

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

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

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

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

****

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

CRYPTO-SCRAMBLE

By Richard Atkinson

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

1. A Y E K I N G P E T E R
   _ _ _ _ Q _ Q _ _ _ _ _
   Orders components.

2. F R A I L P A Y
   _ _ _ _ Q _ Q _
   System statistically diagnosed by the digraphic I. C.

3. B U S T B Y
   _ _ _ Q _ _
   RYE program which does the remainder test.

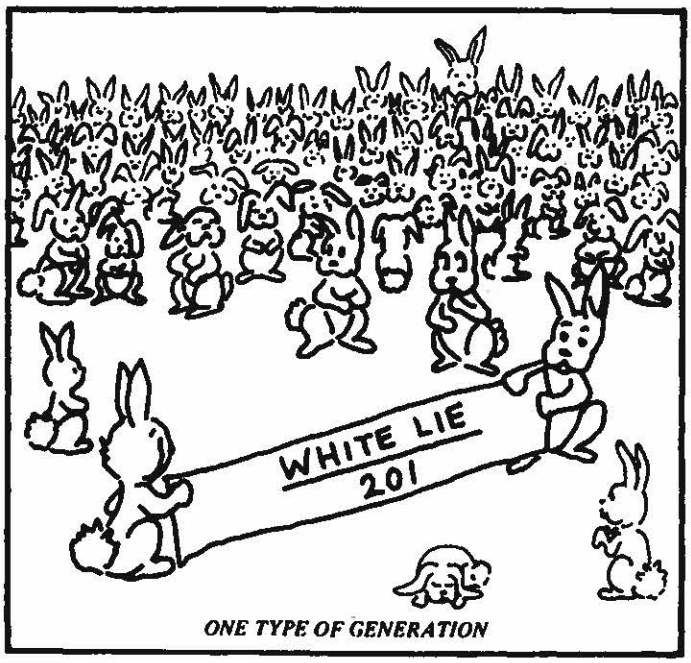
4. E N D C O N I C I C E
   Q _ _ _ _ _ _ _ Q _ _
   A hit.

5. C O D E I R I P
   _ _ _ _ Q _ _ Q
   Cyclic.

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

Print CRYPTOANSWER here.

_ _ _ _ _ _ _ _ _



ONE TYPE OF GENERATION

Answer on page 47.

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

AG-22: WHERE DO WE GO NOW?

by Phil Remsberg, B41

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

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

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

development are only now being explored.

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

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

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

THE DEVELOPMENT OF A COMINT TRANSLATION COURSE FOR VIETNAMESE LINGUISTS

by Jack R. Sharretts, B6

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

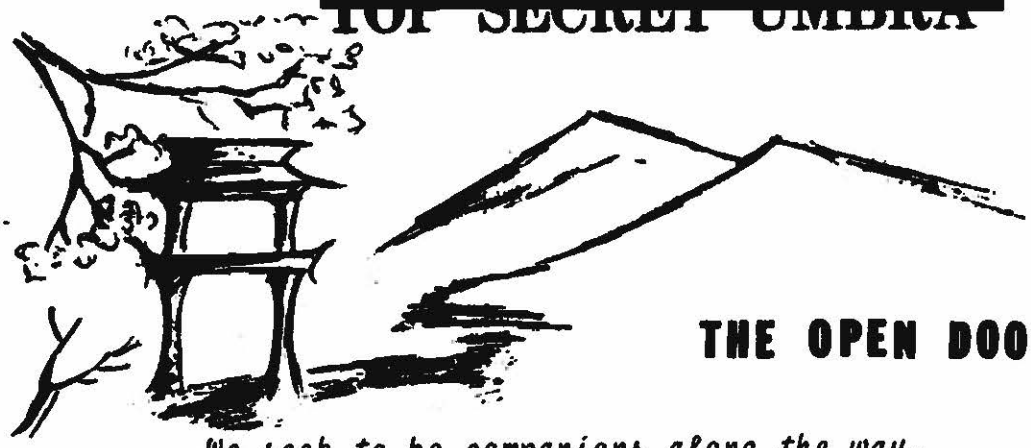
Bloc 9 - North Vietnamese multichannel communications... equipment capabilities and communications procedures...special terminology...translation exercises using transcripts of NVN military and civilian multichannel material.

TRANSPOSITION:

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

NOLIT	EELUR	NBLUE	IHHXC	ATRHH
ADCDE	EODND	RNDOT	IEHCP	XARDU
PSYYA	BAXHW	EFOIA	IBDRH	NBKEM
OAIRR	NVRNF	AENHU	OETIT	NOLXD
NTJAD	VTUSE	VRDNI	NNSOA	TOANN
RSXUI	OMEST	RYNHY	OEISN	FNNXT
DHESD	MHSLF	GOURC	EEECO	HSRAE
ORNOS	SAIRX	LEHIA	AEENW	OSRIE
BDSTC	NITUR	NAABU	LESOS	IFPEA
HMANN	DPAEI	TTMER	UUXGR	EASFF
LWHXE	TNGBR	HRTEI	TXAES	NREEH
IDITL	OHODE	TWTOF	UDTXN	ROIXP
TEFUR	SOHIE	IERSO	THEOE	EGNNH
TNUXD	BNOES	BTUDF	XSMAS	ETSTD
HBFES	NOIRD	ETHNS	SUEDI	ESANS
LTUVM	FCEVR	FRUSF	OTTMG	ASEEA
IAEAE	SLATR	EWOHF	UNWIH	EDANS
DELUE	IDETB	EWTSI	ENGOF	LANII
IENDT	ORNHN	NRCXM	TEPTA	NREAW
AEOUN	RHERO	GHOOO	00013	00487

Answer on page 46 .



THE OPEN DOOR

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

-The Concept of Dragon Seeds

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

by Louis C. Grant, ADPSD

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

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

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

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

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

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

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

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

The Eight Diagrams and Symbol of Creation

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

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

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

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

MACHINE-AIDED TRANSLATION

by Normal Wild, B03

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

Automatic Look-up

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

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

Since WWII, bilingual code groups have been little used. Batches of Laotian Communist political traffic [redacted] were so processed with some benefit. Only code groups for words and phrases were put into English since it seemed over-ambitious to fit together syllabic

streams and to find equivalents on a dictionary tape. The cool reception given to the bilingual code group can arise either from the lack of neat lexical units in the codes--many Asian codes have a high percentage of syllabic values from which poly-syllabic words are composed--or from fear that the English equivalent will be unnecessary to the experienced linguist and a harmful crutch to the inexperienced. But it would be a bit much to say that bilingual code values would not be useful anywhere in NSA.

Bilingual code groups carry a fringe benefit--economy in data preparation under certain conditions. When an entire codebook in encode order is obtained after being abandoned by enemy troops, a decode bank for VMP can be prepared by matching the code groups to the file-maintenance numbers of a dictionary tape and picking up the plain value in the language plus, at no extra cost, its English equivalent. It should be faster and more accurate to input a several-digit file-maintenance number than to input the plaintext value, especially if the native script requires a cumbersome conventional coding. Should such a program be established, the senior linguist in an area would control it. He might assign English values for the sole purpose of indicating standardized translations. It is well to consider that, if bilingual code groups might be useful <u>some</u> time under <u>some</u> circumstances, <u>now</u> is the time to get them ready.

The only place in NSA where full texts are matched against a dictionary bank--in principle, giving English for all the words in the order of their appearance in the text--is the Chinese Communist (PRC) civil problem. Very possibly, the balance of pro and con (as listed in the second article of this series) is more favorable on that problem than elsewhere. There are huge volumes of material which would be machine-processed in any case, mainly for categorization and distribution. The additional cost of finding and printing an English equivalent is fairly small. Much of the material is used for long-term studies, so the processing delays are tolerable. The average Chinese linguist on the job is slowed down considerably by having to thumb the dictionary. He is also troubled by "false friends" (words which do not mean what he thinks they do), by problems in breaking the stream of syllables into words, and by the need to memorize or to look up the telegraphic code for lack of a printout in Chinese script.

The Chinese linguist probably gains somewhat more from an automatic look-up than do workers in other languages. The base form of a Chinese word is not subject to inflection, so there is no problem of removing inflections to find the base. The stream of Chinese characters is represented in plain text by a stream of four-digit numbers, occasionally interrupted by a foreign word or by digits in parenthesis used for their true numerical value, making it "neat" for machine handling. On the other hand, the stream of groups has no indication of word separation and sometimes none of clause and sentence separation, and there is little in the "shape" of the Chinese characters to help. There has to be a program to find words in the stream, and that program would involve some trial and error. Groups of syllables looked up might not turn out to be the true word divisions of the text, and even if they were, the true word-division may not be in the dictionary and a "no match" would ensue in either case.

The PRC Civil program has been used on two unclassified books as an experiment and as a training aid. Since authorized translations of the books are available, a translator can try for himself to see how helpful the program is, and the person who knows no Chinese can see how well he understood the text with the machine version alone.

Much the same program would be applicable to other languages such as Vietnamese which are written or transmitted in syllabic units and have little or no inflection. Thai and Lao are, loosely speaking, monosyllabic like Chinese, but many words of Indic origin are quite long and would not be caught by a four-syllable cut. Korean is poly-syllabic, but it is conventionally written one syllable at a time; the noun has no inflection, but the verb is lavishly inflected. The verb inflection does not always change the form of the verb stem which might still be caught. Cambodian is poly-syllabic but not inflected; if the language is input one syllable at a time, it could probably be handled by such a program. In fact, given a syllabic stream, "the machine wouldn't know the difference," whatever language is used.

There would be some insurance value in a bilingual code program for rare languages, such as some of the minority languages of China, for which there is little or no demand at present. In an emergency, a good linguist would be able to do something with a text, given the printout and some hasty study of grammar.

Automatic "on-call" dictionaries have been used in NSA for Spanish (CAMINO), Vietnamese (RICEBOWL), and French (FRANCOPHONEGLOS). Essentially, the user types in a word or phrase and gets back a definition, either printed out or displayed on a screen. Dictionaries, being merely a particular type of information file, may have to share time with other files, but the automatic dictionary has several advantages over a printed book. Chief among them is that the file can be updated rapidly and often, while a desk dictionary is normally updated once in several years at best. Other advantages are speed in some cases (it may be possible to put in a number of words at a time and get a rapid printout of all the definitions), and various fringe benefits from the availability of the data for machine manipulation. The desk dictionary, however, is always available (no time-sharing, down-time, and rewriting problems) and requires no typing for input. Possibly the best combination is a printed dictionary for well established information and a machine dictionary as a live file to use between editions and for ephemeral information as well as for the fringe benefits.

Responses to CAMINO and RICEBOWL, as machine systems, have been mixed. To many people, they are only a way of getting a hard-copy dictionary--which is by no means a small benefit. Their usefulness as a degarbling and recovery aid depends on whether conditions are optimal or real-life. The quality of the file and its timeliness depend on the people who contribute to and manage it. Of course, the same is true of a card file in a cardboard box; it is easy for a passerby to take cards out of a box and lose them or to write anonymous information on a card. The computer dictionary in some ways encourages good management. Not only is access to the file controlled, but several different people can refer to it simultaneously.

If computer dictionary files do not exist throughout NSA, it may be that they were considered and a thoughtful decision made that they were unnecessary. But maybe not.

****

"Those who have free seats, hiss first."
---Chinese proverb

THE WADE-GILES SYSTEM

by E. Leigh Sawyer, B02

(Author's note: The demands of time have permitted little opportunity to check my memory against primary source materials lending themselves to glossological substantiations. Minor abberations, it is hoped, may be found excusable.)

為無為

For the p'erson who has had little exp'erience with the Ch'inese lankuache, the p'ronouncing of p'lace names, p'eop'le's names, art'ifak't's, and even the inkretient's of Monkolian parpek'ue is often k'onfusing. An unterst'anting of at least Wate Chile's ap'ost'rophic usache aft'er cert'ain k'onsonant's chust might enaple one t'o atchust himself t'o this esot'eric linkuist'ic area. A little pak'ground on Wate Chiles might pe in orter. Wate Chiles was porn in Ch'ik'ako, and lat'er moved to Cheorchia. At that t'ime, his mother atvised him, "You ought t'o invent something. Why ton't you ko t'o Ch'ina, Wate, and invent the Wate Chiles syst'em?" He said, "Poy oh poy, mom, puy me a t'ik'et and I will t'ake the first poat leaving p'ort." So he t'ook off for K'athay. His letters t'o his mother reflek't the choy he felt in t'raveling from p'lace to p'lace. He mate reference t'o the many intichenous t'ype nat'ives he had pump'ed int'o, and the cheokraphik'al ottit'ies he had seen. In any k'ase, as may be kauched py it's witesp'read usache t'otay, Wate invent'ed his syst'em, and it is seen on map's and all k'inds of swell st'uff all over the p'lace.

On the pasis of the k'arefully kathered tat'a p'rovided apove, one k'an easily tecite how t'o p'ronounce that p'art of a Ch'inese p'lace name that has an ap'ost'rophe in it, and one which toesn't - also p'rop'er names (poys or kirls) and telek't'aple Ch'inese tishes such as K'ant'onese st'yle pean k'urd.

T/A-MATH SYMPOSIUM REVIEWED

by David J. Tiren, B61

The September 1972 Dragon Seeds *noted B participation in a symposium on* Mathematics and Traffic Analysis. *David Tiren, B6, attended the symposium and prepared his comments in a stream-of-consciousness format. Because of the B interest in this subject, he offered his remarks to* Dragon Seeds. *He reminds us that they are subjective and do not cover all presentations, but are some of the highlights of the symposium as he remembers them.*

"I attended the T/A and Math Symposium held by P1 at FANX II on 24 and 25 May 1972. A hardcopy transcript will be available ultimately; however, I thought some quick notes and observations might be useful. I won't include all the speakers or even all the ideas of those I will use, but just some of the highlights as I remember them.

Robert Prestel spoke of D7 and some of its operations. As an example, he used a system for choosing an intercept site against a given target, while trying to predict what frequency and schedules the target might use. Over-simplified, it goes like this. Using wave propagation data available through open and other sources, an estimate of the optimum combination of receiving frequency (perhaps in increments of a tenth of a megahertz) and a time (24 hourly increments) is made for a given target station. All the combinations which meet a certain threshold of probability (say 80%) are noted. The same thing is done for the other end of the target link. The intersection of the two sets of data provides all the probable frequency/time pairs the target link will use. The next step is to estimate these probabilities for each potential intercept site. The site whose set of combinations (again, over the same threshold) has the greatest intersection with the set for the target link is the candidate for the task of intercepting the link. The last step in the process is setting up a program for systematic search, the specifics being based on the technical data provided.

Foster Slade, B3, gave some practical examples of a desk analyst employing simple arithmetic to recover aircraft type designators using times reflected in navigational air traffic in conjunction with known airfields. If a given designator, known to represent an aircraft type, is observed consistently in the

context of the amount of time it takes to go a known distance (i.e., we know its speed capability), then it can be only this or that type of aircraft. Once ample data is available, all designators should be recovered. Conversely, if we have all designators but certain airfield cover numbers are unrecovered, we can use the same kind of math to compute the distance from known points, using known speeds/times. If computing the distances gives us a point on the map which is near an airfield, we have made a recovery. Basic, but it is an application of match by an analyst.

Ken Cohen, B45, talked about recovery of three-digit

demonstrated interesting uses of computers to solve topological problems. One of them involved plotting some towns in England, Wales and Scotland. The computer was given a list of the towns and the distances between all pairs of towns, (much like mileage charts on our road maps). The computer then plotted all the relative locations. Since the towns were chosen wisely, the resultant dots on the map formed a rough outline of the island of Great Britain.

A second application was shown by the use of counties. A list of the counties of Great Britain, plus the number and name of the counties on which each county abutted was given. The computer then printed out the name of each county in its relative position. The result was a little distorted because of the great variances in size among the counties. When the technique was applied to the departments of France, the results were phenomenal, as those departments are similar in size.

Caterino Garofalo, P14.

More about Gary later.

Richard Atkinson, P12/E13, appeared in a film produced by the school. The film drew analogies between the Delta Index of Coincidence (I.C.) and baseball batting averages. It was the clearest explanation of I.C. and its uses I have ever seen. Four Stars, rated G.

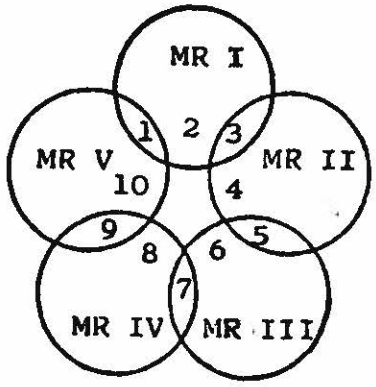
Floyd Taylor, A75, spoke about spherical geometry and its uses in plotting from radar information. Questions from the audience about "Why go through all this geometry when the TALL KING radar is line-of-sight gear?" left this subject sort of up in the air.

William Binney, A72, gave a very elementary example of the application of Set Theory in a context where most analysts would consider it an intuitive thing. The example assumed complete knowledge of a callsign system so that a given call could be identified as coming from a given book. The example showed several "Military Regions" and their book usage.

	SET	A	B	C
Region I	(Book)	1	2	3
Region II		3	4	5
Region III		5	6	7
Region IV		7	8	9
Region V		9	10	1

(Sets represent certain date periods)

Intuitively, we say that a callsign from Book 2 is (was) used only by MR I, while Book 5 is either MR II or III. This can be presented in a Venn diagram:

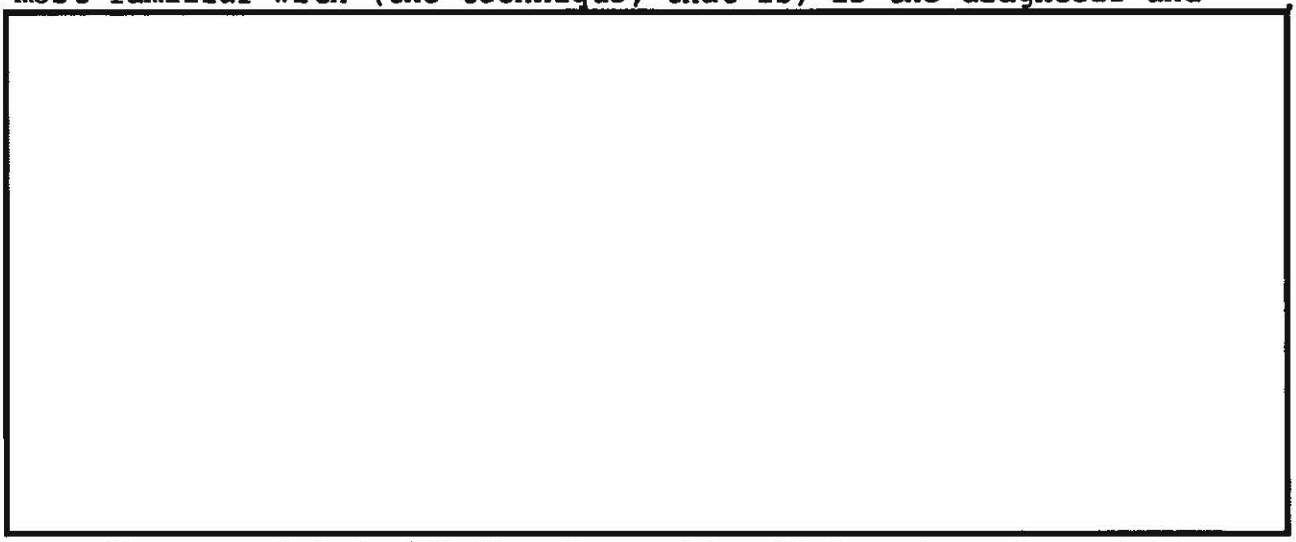


EO 3.3b(3)
PL 86-36/50 USC 3605

Again, very basic, but an application not usually considered in the realm of math by the layman.

Dr. Reed Dawson, P12. Dr. Dawson's lecture on Set Theory and Probabilities was addressed to the problem of trying to determine how much of the total traffic transmitted we actually intercept. Sorry I can't go into more detail because the math was not intuitively obvious to the casual observer.

The last speaker was Gary again. This time he gave illustrations of actual Soviet problems of the early 1950s. The one I'm most familiar with (the technique, that is) is the diagnosis and



Gary concluded with the observation that we have been doing analysis for a long time. He wondered if we were dealing with new concepts (math applied to analysis) or just new names of techniques.

I guess the real impression I got from the symposium was one of re-emphasis on the idea that not many of the cryptologic disciplines are pure. We are always applying whatever talents we have to the job at hand and don't worry too much about names or titles some people apply to the things we do. But it is refreshing to find again that many of the disciplines are not steeped in "Black Magic," but are based on common sense and basic knowledge of how things work. I think, the next time one of my analysts complains about routine, so-called "flunky" work, I'll try to impress upon that analyst all the different, ostensibly esoteric, techniques that are applied on a routine basis."

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

----Grids for the new positions of the B forward outpost relocated to FANX II from FANX III on 20 November 1972 are: A2540--B1, A2E72--B11, and A2548--B12. Operating frequencies are unchanged.

****

----Employee recognition: "All of you who are supervisors, especially, take care of your people. Recognize their work. Let's do all that we can to reward their performance." This quotation from Lt Gen Phillips's opening remarks on assuming the Directorship should be noted by all supervisors regardless of their position in the chain of command.

The Agency's Incentive Awards Program provides one means of recognizing employee accomplishment. For many personnel, "Employee Suggestions" are synonomous with the entire awards program; most frequently they are unfamiliar with its many other aspects.

Visible evidence of the variety of employee awards--cash and honorary--sponsored by NSA was recently on display in the passageway between Gatehouse One and the Operations Building, and in the case on the south side of the Operations Building, 1st floor escalator. All personnel, especially supervisors, are encouraged to become familiar with the numerous awards which are available to recognize employee accomplishment.

The NSA Personnel Management Manual, Chapters 503 and 504, identifies these awards, outlines eligibility criteria, and advises on procedures for initiating and submitting recommendations. Information and assistance are also available from the Incentive Awards Branch (M362), Room 1A190.

****

----Speeders beware! MPs at Ft Meade are using a "Buck Rogers" contraption to measure auto speed. It is hand-held, can operate from a patrol car battery or portable battery pack, and is accurate to one-tenth of a mile per hour. The radar gun sends a radio signal to the observed car. The signal bounces back and the speed is indicated to the MP operator.

****

----The NSA International Affairs Institute is trying to obtain George F. Kennan of Princeton to open the 1973 lecture series. Other speakers being sought for 1973 are Charles Bohlen, Arthur Schlesinger, William Buckley, one of the Rostow brothers, Zbigniew Brzezinski of Columbia, K. Galbraith, and Admiral Kidd (ex-Commander of 6th Fleet). The final lecturer of the 1972 series will be a U.S. diplomat speaking on Latin America (probably Chile).

The Institute has started to explore the feasibility of implementing its other objectives, i.e., SIGINT report writing and SIGINT seminars. Since the matter is somewhat complicated, could we ask the readership of *Dragon Seeds* for ideas on these two goals? Incidentally, IAI member Dick Seron of B6 has already presented his views on seminars; possibly other readers have something to contribute.

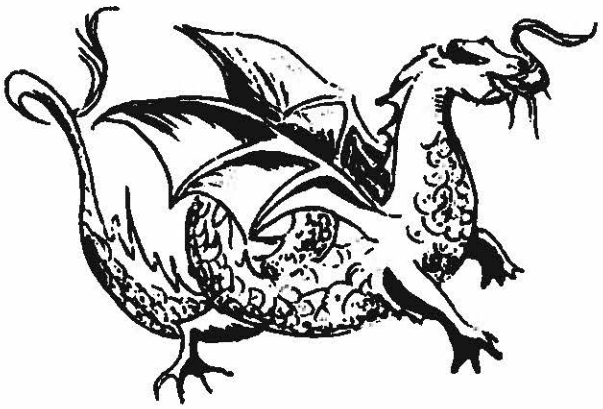
Our membership drive for 1973 will begin the first week in December. Since the type of lecturers depends largely on what we can offer as honorarium, we are seeking increased participation. Dues of $3 per year may be forwarded by check to Mr. James Duncan, P1. Be sure to include your name, organization, and both telephone extensions.

****

---B Group cryptanalysts should be wary of the STET program included in the IBM 370 RAPIDS package. During her recent tour in B1203, Dr. Marti Branstad identified serious errors in the polygraphic repeats portion.

****

Behold the turtle! He makes progress only when he sticks out his neck.



ASK THE DRAGON LADY

Dear Dragon Lady:

What are the views of the TACP on changing jobs to benefit from points awarded for experience?

--An Aspirant

Dear Dragon Lady:

Why does the TACP not accept applications for the TA Intern Program if they have had more than two years cryptologic experience? The selection criteria referring to experience states, "...must ordinarily have at least one year of TA experience at minimum GGD-07 or E-5 level; however, must not have more than two years of cryptologic experience at GGD-07/09 levels." (See OM, Subject: NSA Intern Program Vacancies, dated 28 August 1972.)

--Piqued

The Dragon Lady asked the Executive of the TA Career Panel to comment on the above questions. His views follow:

Dear Aspirant:

The TACP has recognized that there are benefits to be derived from exposure to different types of targets, and has specifically organized its PQRS to encourage movement of TA aspirants between different TA problem areas. Bonus points are awarded in one lump sum of 140 points for a second exposure; this implies that the first exposure consisted of

at least one year at the GGD-07 level or military equivalent or at the GGD-05/E-4 levels where it can be shown that this experience equates to the higher grades. Point values for TA experience are allocated at the rate of 15 points per month for the first two years of creditable experience, 10 points per month for the third year, 5 points per month for the fourth year, and 2 points per month for the fifth, sixth, and seventh years. The declining point allocation is intended to prompt rotation to gain diversification on another problem, e.g., if an individual remains on the same problem (same category of creditable TA experience) for seven full years under the present criteria, he can accrue only 612 points of a possible 750 maximum. One year in another creditable experience category would gain him the 140 bonus points or maximum in experience. A revision to the criteria is currently being typed which allows more points for the fifth, sixth, and seventh years of TA experience and broadens the exposure areas for bonus awards. Watch for the revision, which will be on the streets hopefully before the first of the year.

****

Dear Dragon Lady:

I am writing to express my feelings about the various informal prep sessions held prior to the CA PQE. As you are probably aware, these sessions are given by A, B, and G to acquaint their personnel with the types of questions contained in the exam. When one considers the logistics involved in staging three separate sessions, the mind boggles. For example, regardless of the length of the class (less than 30 hours for B, and more than 200 hours for A), you still have three classroom facilities, three sets of study materials, and three sets of instructors.

Enter my theory: I would like to suggest a single prep class, sponsored by the CA Career Panel. This class would be open to all persons eligible to take the PQE regardless of group affiliation. One of the benefits of this would be the elimination of two classroom facilities, two sets of study

materials, and two separate sets of instructors. Another benefit is that the CA Panel has access to the best qualified instructors for any given phase of problems, and knows the material which will be contained in the exam. Then, personnel in B or G, who currently spend less than 50 hours on preparation, will not be any less prepared than personnel from A, who currently spend more than 200 hours in preparation.

Respectfully,

MORRIS L. FERGUSON

Dear Morris:

Mrs. Wilma Davis, CACP Executive, tells us that the Panel views provision of training for non-interns as a proper function of line management. The Panel evaluates PQRs submitted by individuals and recommends specific training courses that would be of value in pursuit of professionalization. To that extent, it provides individual help in preparation for the PQE. The CACP does not involve itself in actual teaching, but has provided teaching materials and suggested study aids to organizations and individuals as special help in preparing for the exam.

We asked the same question of three other career panels which include a PQE in their certification procedure. The Traffic Analysis Panel looks with favor on the offices' providing such training and has supplied material for their use. Like its crypt counterpart, the TA Panel does not itself engage in teaching. The Special Research Panel considered our query a bit premature, since the PQE for that field is still being evaluated. The SR Panel does intend to provide to individuals preparing to take the PQE a study guide which will be available to them about two months before the date of the exam. The main concern of the Data Systems Panel is at present its interns, but it is considering the possibility of providing special help to non-interns getting ready for the PQE.

To Virginia and Meech, who asked, "How do you get a job on a career panel or in its executive office?"

Again, our source of information is Mrs. Wilma Davis, CACP Executive, who tells us that Panel members and the Panel Executive are appointed by ADPM upon recommendation of the Panel Chairman. The two technical assistants to the Executive are appointed by the Panel and serve for two years. They, like the administrative and clerical assistants, are attached for administrative purposes to the organization to which the current Chairman of the Panel is assigned. A vacant assistant job may be filled by advertising or by inter-organizational transfer. If you are interested, you may want to talk to the panel Executive.

****

"Please let me see my article in Dragon Seeds..."

SOLUTION:

G L I M P S E S O F T H E S A G E S O F C H I N A

9 15 13 16 20 21 4 22 18 7 25 11 5 23 1 10 6 24 19 8 3 12 14 17 2

C O N F U S I U S M A I N T A I N E D T H A T G O

O D G O V E R N M E N T O B T A I N E D W H E N T

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

S T E R M I N I S T E R X W H E N T H E F A T H E

R W A S F A T H E R A N D T H E S O N S O N X T H

A T S O C I = E T Y W A = S A N O R = D I N A N C

E O F H E A V = E N A = N = D W A = S M A D E U P

O F F I V E R E = L = A T I = O = N S H I P S X X

R U L E R A N D S = U B J E C = T H U S B A N D A

N D W I F E F A T H E R A N D S O N E L D E R B R

O T H E R S A N D Y O U N G E R A N D F R I E N D

S X X R U L E S H O U L D B E I N R I G H T E O U

S N E S S A N D B E N E V O L E N C E O N T H E P

A R T O F T H E F I R S T F O U R X S U B M I S S

I O N T O R U L E S H O U L D B E M A R K E D B Y

R I G H T E O U S N E S S A N D S I N C E R I T Y

X X B E T W E E N F R I E N D S X T H E M U T U A

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

E T H E G U I D I N G P R I N C I P L E X X O F A

H E R E A F T E R X H E D I D N O T T E A C H X X

Z_1 and Z_0 are non-textuals: the first contains the number of unused cells in the matrix and indicates the key column under which the diagonal (comprised of the first four groups of cipher) was extracted. The second non-textual contains the group count of the message.

****

Answers:

1. Repeating key
2. Playfair
3. Stubby
4. Coincidence
5. Periodic

Cryptoanswer:

Fibonacci

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

CONTRIBUTORS

WALTER D. (JOE) ABBOTT, JR., B605, received his B.A. in English literature from Harvard College in 1960 and entered the Army Security Agency shortly thereafter. Among his Army experiences were a year in Monterey studying Chinese-Mandarin and a two-year tour in the Philippines as the OIC in the Processing and Reporting shop for the now defunct USM-9. He joined NSA in 1966 and had a tour in Hawaii, during which time he was the NSA Pacific representative to the CINCPAC IGC working group. A certified Special Research Analyst, he is currently the Chief of the Intelligence Staff for all Communist Ground Force activity in Southeast Asia.

JEAN F. GILLIGAN, B32, was graduated from Duquesne University, Pittsburgh, Pennsylvania and pursued graduate studies at Catholic University, Washington, D.C. She entered on duty with NSA in December 1968 with the PRC [redacted] Division Intelligence Staff. Mrs. Gilligan is presently assigned as the acting chief of the [redacted] Section of the PRC [redacted] Branch. She is responsible for the entire production of the PRC [redacted] as well as research and reporting of PRC [redacted] activity.

TOM GLENN, Chief, B61, has a total of 14 years experience with ASA and NSA on the Vietnamese problem. He is a professional Special Research Analyst and Vietnamese linguist who has also studied Chinese and French on his own. Mr. Glenn has served as the Chairman of the Vietnamese Language Professionalization Examination Committee. Assigned to Vietnam in 1962-65, 1967-68, and 1969, he has been involved in traffic analysis, cryptolinguistics, intelligence analysis, and most significantly, in the management of the SIGINT reporting effort on the Vietnam war.

LOU GRANT is a professionalized Special Research Analyst with over 22 years Agency experience. He spent the first 15 years on B Group problems, working as a traffic analyst, reporter, and staff officer. Since leaving B Group, he has served as an Assistant Inspector General, Administrative Chief for NSA Europe, and is now an Action Officer in ADPSD.

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

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

E. LEIGH SAWYER, Chief of B02, majored in Romance languages as an undergraduate at Harvard, and attended the Chinese Language School (Hua Wen Hsueh Hsiao) at the University of California Berkeley while in military service. He subsequently served with a Chinese Army Command in Nanning until VJ Day, and left China in 1947 following G2 and Assistant Military Attache assignments in K'unming, Shanghai, and Nanching.

JACK SHARRETTS, B603, joined the Agency in 1962 after receiving his Bachelor of Music degree from the University of West Virginia and completing a six-month tour in the Army Reserve in which he served as a Munitions Transshipment and Storage Specialist. Hired by the Agency as a cryptanalyst on the Soviet [redacted] problem, he shifted within six months to B Group and a Vietnamese translation course. His ten-year tour as linguist, cryptanalyst, and reporter in various B6 elements has been highlighted by assignments to the NVN Navy problem, Civil and Diplomatic problem, and a TDY to Phu Bai on VC Tactical Military and General Directorate of Rear Services problems. In B603, he is primarily concerned with the training and assignment of linguists in B6 and the maintenance of RICE BOWL, the computerized Viet-English dictionary.

DAVID J. TIREN, B61, plied the trade of ASA intercept operator for six years. He accepted a position in the original NSA Civ Op program, serving in Kyoto, Japan, for two years in the late fifties. Later, after six years as a Traffic Analyst in A6, he spent 1964 as a member of Class Five, CY-100. Assigned to B6 in early 1965, Mr. Tiren has had a variety of exposures and emphases. He is currently Chief, B612, a branch whose responsibilities in the North Vietnamese non-Morse communications area include tank-to-tank communications (see September DRAGON SEEDS).

NORMAN WILD, B03, is one of the Agency's foremost multilinguists. He has been with NSA and predeccessor 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.

it's

classified!!!