

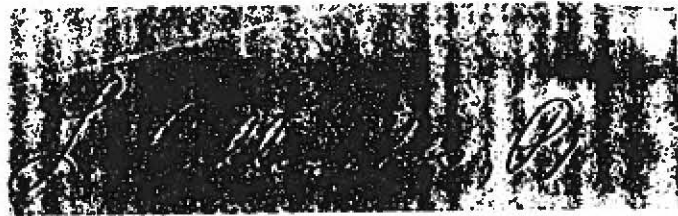
~~TOP SECRET~~

National Security Agency
Fort George G. Meade, Maryland



DECEMBER 1973

**DRAGON
SEEDS**



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~TOP SECRET UMBRA~~

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~~

DRAGON SEEDS

Publisher

DONALD E. MCCOWN, CHIEF B4

Managing Editor
Minnie M. Kenny

Executive Editor
Robert S. Benjamin

Rewrite Editor
Jane E. Dunn

Special Interest Editor
Ray F. Lynch

Feature Editor
Robert F. Kreinheder

Education Editor
Marian I. Reed

Composition

Louella M. Ertter

PRESS CORPS

B11	Carolyn Y. Brown	B42	Peggy Barnhill
B2	George S. Patterson	B43	Mary Ann Laslo
B31	Jack Spencer	B61	<input type="text"/>
B32	Jean Gilligan	B62	Edmund J. Guest
B33	Louis Ambrosia	B63	William Eley
B41	James W. Schmidt	B65	Philip J. Gallagher

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



VOL 2
NR. IV

DECEMBER 1973

TABLE OF CONTENTS

Chinese Communications Developments..... Jack L. Thomas 2

1972-73: A Viet Nam Odyssey...Leo Stepp & Edward O'Connor 8

Christmas at the School..... Morris L. Ferguson 17

Time to Look at People..... Tom Glenn III 19

The Open Door: Are You Using Computers?...Dr. Walter Jacobs 21

Minnie's MINI..... Minnie M. Kenny 23

B Needs Its Own Computer..... William P. Stivers 24

[Redacted Box] Russ Myers 31

Seedlings

Ask the Dragon Lady *

Contributors

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

With this issue, DRAGON SEEDS marks its second anniversary. I am pleased, on behalf of all of B Group, to extend to its publisher, editors, press corps, and contributors congratulations and thanks for making it a successful and useful publication. We have all benefitted from your efforts.

DRAGON SEEDS has demonstrated its worth as a valuable means of exchanging information among people in B. For analysts and technicians, it has provided an outlet -- a means to share ideas, to tell others of successes, to learn about new or different techniques, to express concerns, and to ask questions. For others, it has given a new understanding of operational problems, highlighted additional areas of interests and offered some new perceptions on how we go about our business. It has made us aware of important developments not otherwise publicized. For all of us, DRAGON SEEDS is informative; it invites us to think; it helps us to do our jobs better.

We all should work to see that DRAGON SEEDS continues to serve us well. With our continued interested support and willingness to contribute articles, it will remain a relevant and useful way to share operational and technical ideas within B Group.

Happy anniversary, DRAGON SEEDS!
May you continue to instruct, inspire, and provoke us.

Wm C. Jackson

~~TOP SECRET UMBRA~~

CHINESE COMMUNICATIONS DEVELOPMENTS (Where Have They Been, Where Are They Going?) by Jack L. Thomas, B44

*There is high technology in China today. Indeed, it would be fair to speak of an electronic revolution in many fields.**

This statement will undoubtedly raise eyebrows of a number of readers and trigger the response: which China are we talking about? Certainly not the People's Republic of China? But we are talking about the PRC. And the statement for the most part coincides with beliefs held by the handful of Chinese "technique watchers" who have followed evolving PRC communications developments and trends throughout the years.

But how did the Chinese reach this point so suddenly, apparently without our knowing about it until only recently? The answer is that they, of course, did not reach this point suddenly, nor recently. It has been evolving over a number of years, and generally speaking, we have been aware of it. What the Chinese have denied us over the years has been the detail needed to tie the bits and pieces into an overall China-wide picture. Their penchant for security, bordering on national paranoia, is well known to analysts who have followed the problem from any standpoint throughout the years, and this pertains to the communications technique watchers as well.

This is not to say, though, that these analysts were totally blind to the overall picture that was evolving, nor were they totally without information to predict specific developments which later often proved highly accurate. Documentation exists that will substantiate accurate reporting on developments and trends in many areas of the Chinese communications establishment. These predictions, however, were of necessity frequently general, having as their basis a variety of sources which were often too anemic, too sparse, or too tenuous to permit their being pieced together into a picture showing precisely what the Chinese were doing, or where they were headed. Nor in many cases were they sufficient to permit detailed statements of specific PRC communications developments and trends that could be defended to the degree necessary to justify planning and programming actions.

**From "High Technology in China," Scientific American, December 1972, by Dr. Raphael Tsu, an IBM physicist who extensively toured Chinese factories, universities, and research centers in the summer of 1971. (See the Summer 1973 issue of the Cryptologic Spectrum for a review of this article.)*

~~TOP SECRET UMBRA~~

Though in many instances analysts watching the problem daily could sense probable future developments, they were often hard-pressed to document their beliefs. These analysts were of necessity a cautious group. They had to be, given the paucity and shakiness of their sources, the scope of the problem confronting them, and the rareness of their species.

In addition to their strict adherence to security, the Chinese further frustrated analysts throughout the years by displaying amazing talent for being unpredictable. They would surge forward in certain areas, apparently determined to pursue these avenues to satisfactory conclusions. But as analysts began to predict future trends on the basis of these developments, the Chinese frequently (and often without apparent reason) changed their course, or in some instances stopped development of a particular technique or system and showed no apparent future interest in it. Especially perplexing was the fact that some of these efforts afforded the Chinese distinct advantages, far outweighing other courses of action, and in many cases seemed ideally suited to their particular needs. Nor did they always develop their communications along lines considered advantageous by Western standards, though in many areas the technology involved was almost certainly available to them. But we should also keep in mind that what seems to us to be aberrations in Chinese developments, may stem from either a lack of consensus among their planners on long-range goals, or our inability to share their perspective on long-range goals.

This is not to say, however, that Chinese communications developments were stagnated during the years, or showed no sustained advances. Far from it. The PRC has long considered communications and electronics to be high on its national priorities list. Consequently, internal disturbances such as the Cultural Revolution apparently did not slow research and development significantly in this area, as was also apparently true of other high-priority areas. And when the situation the Chinese inherited in 1949 is additionally considered--amounting to an almost non-existent communications capability decimated by years of war and few factories capable of producing needed equipment and systems--they have done quite well indeed. This is all the more noteworthy when one also considers the almost total cutoff of Soviet technical aid to China in 1960, and, until recently, difficulties the Chinese encountered in obtaining technology, equipment, and systems from the West because of trade embargoes and restrictions.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Discussing how to improve their motors



Workers of the Electric Appliances Repair Shop have made this equipment to produce silicon elements

~~TOP SECRET UMBRA~~

At the same time, however, the Chinese have not totally been without Western help, nor did the Sino-Soviet rift totally stop their progress. By 1960 the Soviets had given them a solid base upon which to expand--from components, equipment, systems, and technology to whole factories. This Soviet assistance, coupled with the considerable quantities and varieties of equipment and technology not subject to Western embargo, enabled the Chinese to leap perhaps as much as 10 to 15 years ahead of what otherwise probably would have been the case. Additionally, the Chinese learned a valuable lesson from the Sino-Soviet rift and from the difficulties of acquiring assistance from the West. From about 1960 they increasingly turned, of necessity, toward self-reliance in this and other highly technical fields.

But much of the equipment and technology gleaned from the West was not the most sophisticated, by world standards, at the time they acquired it, and it was by and large limited to components and specific equipments. Large and complete systems and the factories to build communications items were almost totally denied the Chinese by trade restrictions. But the technical aid the Chinese did receive nevertheless represented significant steps forward for them and gave them technology and equipment that could be copied, produced, adapted to their particular needs, and used operationally--and in some cases, later improved upon as well. Foreign equipment and technology afforded them the sorely needed base upon which to build their communications establishment--through copy, modification, and domestic manufacture. And although Soviet technical aid was severed in 1960, the equipment, systems, and technology acquired from the Soviets before the rift served the Chinese well for years to come.

The rest the Chinese for the most part apparently accomplished on their own, displaying along the way their well-known ability to "make-do" with what they had available, and leaving the acquisition and employment of sophisticated technology to follow in due course, after basic needs had been satisfied. Through this process, and through increasing interest in more sophisticated techniques in recent years, the Chinese have developed their communications establishment to the point where today it can be said to be capable of supporting the basic needs of the nation.

One word of caution: the Chinese may--and probably do--have technology and equipment of higher sophistication and in greater quantity than they have been given credit for. As noted previously, no target nation has in the past revealed less about its technical progress. Fortunately, however, we have been able to learn something additional about Chinese design and production from captured

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

equipment in South Vietnam, some of which Agency engineers compared favorably with the latest Western technology in this area. But surprising as this was, even more disturbing was the fact that certain of these equipments had been available to the Chinese military in considerable quantities years before they were captured, and that we had no previous information whatsoever about them. Their existence was a total surprise, and so was their degree of sophistication. Nor are these probably isolated examples; there is little doubt that the Chinese have developed tactical--and other--equipment and systems incorporating high-quality design about which we are unaware, and about which we may not become aware except in contingency operations or a national emergency.

Having developed a communications system capable of supporting the basic present-day needs of the country, where are the Chinese headed in the future?

The recent and dramatic rapprochement with the U.S. and other Western nations, coupled with Chinese determination to advance rapidly as an industrial power, will call for sharp increases in both the quantity and quality of communications facilities--both internal and external, both radio and landline. At the same time, slackening of trade restrictions will make advanced Western technology, equipment, and systems increasingly available to the Chinese. And they seem determined to avail themselves of them to quickly bridge present gaps--not just single sets and components that they can copy and produce, but entire systems as well, and in some cases factories to produce them. They now state publicly that they are in fact after entire systems and factories to the limits their economy and foreign exchange will permit, and that they want them as fast as they can be acquired. There is little doubt that they will get them, and that the Chinese will insist on, and will receive, varieties incorporating the latest technology.

This availability of advanced Western technology and equipment, combined with their own rapidly expanding domestic design and production capabilities, point toward solid future Chinese successes in these and related areas. Also to be kept in mind: China, like other Communist countries, can concentrate tremendous effort on areas of national priority, and communications and electronics advances could therefore occur at a faster rate, and at higher levels of sophistication, than present information may indicate.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

In conclusion, the Chinese are on the threshold of an electronic revolution, and within the next decade will demonstrate technological progress that will place it among the advanced industrial powers of the world in this and other highly technical fields. Chinese communications and electronics developments in future years will, therefore, become an increasingly interesting and challenging problem to follow, steadily becoming more complex, but at the same time providing more--and more reliable--material to our analysts, thanks to the "opening up" of China. This situation will place increasing demands on those in the Intelligence Community responsible for keeping abreast of such developments, and on those at NSA, where we like to keep ahead of them.

Yuhsien County workers produce coal tar, gasoline, diesel fuel and asphalt with simple equipment they made from waste materials.



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

1972-73: A VIET NAM ODYSSEY

by Leo C. Stepp and Edward A. O'Connor, F46

Approximately 125 kms SSW of Saigon, four hours by bus, six and one-half hours by cyclo, two tanks of gas by Honda, and forty minutes by Air America "Gooney Bird" in Phong Dinh Province, Central Mekong Delta, lies the beautiful tropical splendor of Can Tho City and sanctuary/hide-away for IV Corps' ruthless, intrepid U.S. Advisory Team.

It was the Lunar Year of the Rat when the Odyssey began. The mission was to advise South Vietnamese Army (ARVN) personnel while they assumed the U.S. SIGINT mission in the delta from USM-607. Since there was no established precedence to follow, each problem encountered had to be dealt with in a unique manner. Realizing that extensive changes were essential to make the transfer of responsibility efficient, the first priority of the advisors was to circumvent the inherent language barrier and to establish a workable rapport with their ARVN counterparts. This was achieved, to some extent, through patient guidance and constant interface, i.e., sign language, graphic illustrations, etc. With such techniques at their disposal, advisors began to examine the innumerable problem areas.

Initial corrective efforts were directed at security procedures which were almost non-existent. The following aberrations were rectified immediately: first, there was no ARVN officer on duty during weekends or holidays; second, an excess of defunct classified material was stored in file cabinets and boxes; third, and most important, ARVN personnel were not familiar with the use of the numerous incendiary devices for the emergency destruction of crypto-gear and classified documents. In addition, advisors established a picture badge identification system and access list for all authorized personnel. This list excluded one unidentified, indigenous individual who purportedly was employed by the 335th Radio Research (RR) Company to guard the antenna field.¹ Although the unit (335th RR Co) departed, Nguyen (???) remained vigilant as ever, at the expense of an unknown source.

Concurrent with improving security practices, a program to extend Manual Morse intercept capability was implemented. Vietnamese operators had and were continuously receiving

¹. Can Tho Centers antenna field is located in a non-secure area approximately 500 yards NE of the operations bunker.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

training in intercept techniques, but their proficiency was far below that of their U.S. predecessors. Specifically, their copying speed was approximately eight words per minute, they could not backlink activity, and they were unaware of the effectiveness of Morse operator characteristics analysis. After discussing these problems with the ARVN commanding officer (CO), advisors received permission to reorganize and supervise the training program. The new program was successful enough, so that the supervision was eventually returned to the ARVN's. When new personnel arrived, they assumed their duties with a minimum amount of on-the-job training (OJT). However, after several months the operators, as well as other personnel, began to lose their incentive. To eliminate this negative attitude, the ARVN CO was convinced to initiate a "Soldier of the Month" award. This consisted of 5,000 Piaster (provided by the advisors) and a Letter of Recognition. By U.S. standards the award was minimal, but the ploy worked. The competitive spirit between sections increased; and following the first presentation, all personnel were striving to achieve this award.

The first award was presented to the Airborne Radio Direction Finding Ground-to-Air radio operator. Significantly, the ARDF tip-off function had undergone an extensive transformation and emerged from a state of chaos and confusion to the point of receiving special recognition. In fact, standard operating procedures were produced by this section and disseminated for employment throughout South Viet Nam.

Following the cease-fire and associated withdrawal of American military personnel, the U6A ARDF aircraft assigned to the U.S. 146th aviation company were transferred to Saigon. Although four missions were tasked from Saigon daily numerous problems occurred and approximately one mission per day was flown. Believing ARDF effectiveness could be increased with additional missions, advisors clamored for the assignment of ARDF aircraft at Can Tho Center (CTC) and the accompanying requirement for preparation of tech data lists (TDL's) for each mission. When four U6A's were finally returned to Can Tho, the ARVN's did not possess the sophisticated secure air-to-ground voice communications as American predecessors, and relied solely on the much slower process of one-time pads. Nevertheless, with Can Tho assuming control of the aircraft and providing mission tech data, ARDF results began to improve and personnel were instructed in methods of altering mission frag points to maintain greater cognizance on priority targets. As a result, more information was provided traffic analysts, enhancing development efforts.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

In the early stages of the Vietnamization improvement and modernization (VIM) Program, there were only five analysts assigned to the T/A section; two of which were radio operators for ARDF ground-to-air tip-off. The remaining three were required to devote all their time to preparing and transmitting daily TECSUMS. To increase productivity, five additional analysts were transferred to CTC, but they had only recently completed school and were unfamiliar with operations. Complicating this situation, the new people spent almost three months painting, filling sand bags, and satisfying other administrative trivialities. When they were finally released to operations, their training was accelerated. In March 1973, the procedure for filing tech data was altered, a new system to handle unidentified entities was established, and the TECSUM format was revised to facilitate changes. Once analysts overcame their fear of error, development was successful and new entities were notated and forwarded as isolated.




Although positive results were being attained, a recurring difficulty plagued the TA section: the perplexing importance of serialization (NR's) and chatter extracts and the necessity for accurate logging of all entries to satisfy a computer -- an alien wonder they had never seen but were told existed. In addition to the lack of experience and comprehension, only one traffic analyst spoke English and he was hospitalized with pneumonia for three months during this critical period. Instruction (pointing and drawing illustrations) was provided through non-analytic interpreters and with the limited operational Vietnamese of the advisors. After many hours of frustrating and occasionally humorous guidance (on the part of both advisors and ARVN personnel), periodic checks of the TECSUM and raw traffic indicated a continued improvement and a decreasing error rate.

Similar complications occurred with exploitable message reports (EMR's) in the cryptanalysis section. Lack of experience again was a prime detriment and initially no exploitation was performed. Personnel only logged and forwarded EMR's from the three ASTD's.² Once the C/A shop was expanded to twelve analysts, a training program (basic cryptanalytic techniques) for exploitation and identification of messages was instituted. Since the ARVN's readily adapted to the program and acquired the basic skills rapidly, one man was sent TDY to each ASTD to establish similar programs of instruction. Eventually 90% of low-level voice intercept was identified, new cryptosystems were isolated and forwarded, and local commanders received required perishable intelligence.

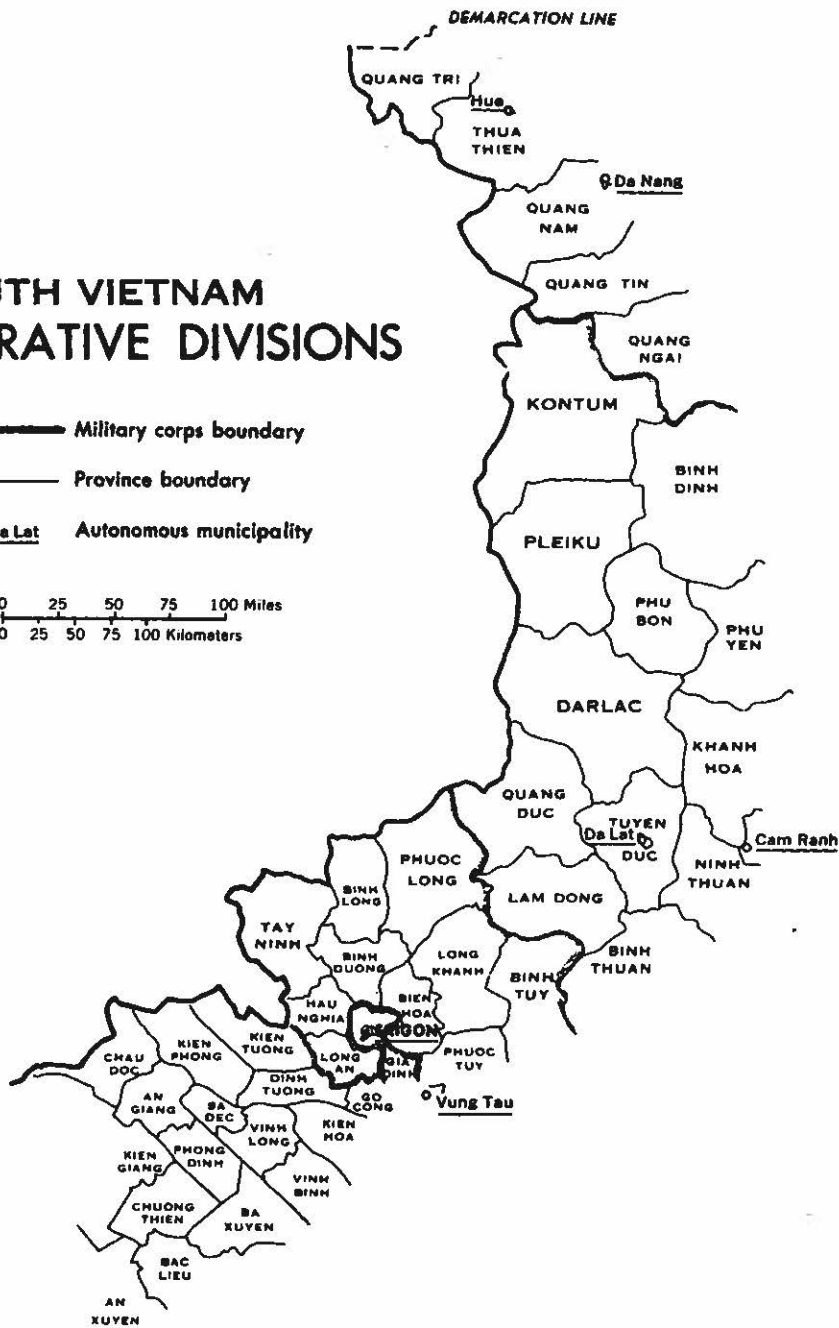
2. ASTD expands to ARVN Special Technical detachment.

~~TOP SECRET UMBRA~~

SOUTH VIETNAM ADMINISTRATIVE DIVISIONS

-  Military corps boundary
-  Province boundary
-  Da Lat Autonomous municipality

0 25 50 75 100 Miles
0 25 50 75 100 Kilometers



DAO PHU QUOC (KIEN GIANG)

CON SON
(Administered from Saigon)

6-72

~~TOP SECRET UMBRA~~

Although results were favorable, there is no implication intended that the cryptanalytic effort was without its peculiar headaches. Numerous problems were experienced in couriering intercept from LLVI teams and from ASTD's when circuit outages occurred. Since the situation vacillated in direct relationship to the tactical environment, advisors were stymied in endeavors to alleviate this dilemma. Despite the requirement, air transportation (helicopter) was seldom available and courier by road was extremely hazardous. Yet LLVI teams attempted courier every two-to-three weeks and when necessary even traveled by bus in civilian clothes. Without any secure means available to transmit intercept for preparation of EMR's, these methods were the only alternatives to satisfy demands for timeliness.

Although timeliness is an innate characteristic of the SIGINT mission, natural and man-made phenomena often alter the course of events. An excellent example was the selection of a location and construction of CTC's AN/TRD-23 medium range direction finding (MRDF) site. Between July and September each year, the tropical monsoons visit Can Tho. Again, field expediency dictates "nothing shall be wasted" (to include monsoons); therefore, concurrent with the arrival of the monsoon was Can Tho's Annual Aqua Festival". Although these festivals improved morale and helped solidify relations with the local inhabitants, the "Year of the Rat" proved to be the last of the aquacade follies. In May 1972 land surveyors from Engineer Region IV (ER-4) inspected the only possible location for Can Tho's proposed MRDF site, which unfortunately, was one and the same as "mini-lake" where the festivals were held. The surveyors estimated that approximately 7,000 cubic meters of fill dirt would be required to displace and remove all the water from "mini-lake" so that a base for the site could begin.

All of these calculations led to numerous questions (not to mention where next year's Aqua Follies would be held): "Where would this amount of dirt be found?"; "Once found, how would it be transported to the proposed site?"; and finally, "Who would finance the venture?"

Because this MRDF site would be an integral part of the ARVN MRDF net serving all of South Vietnam and would be manned by ARVN personnel, it was automatically assumed that the ARVN's would make all financial and building arrangements. After two months of ARVN procrastination, paper shuffling, and overall apparent apathy, the advisors decided to initiate some action.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

There were two weeks of rambling over the countryside in a jeep, over roads previously traveled only by reconnaissance teams. Then the advisors found a large "farm-like" residence, with an expanse of adjoining land. After several hours of verbal ping-pong, threats, shouts, obscenities, and finally handshakes, the advisors had bargained with the owner for the required amount of fill dirt. The nominal fee agreed upon was eight 55-gallon drums of gasoline (hopefully provided by Uncle Sam) and six cases of American beer (provided reluctantly by the advisors from their very limited personal cache).

The fill dirt dilemma was solved; transporting it from the farm to "mini-lake" was still another predicament. After several sociable evenings with members of the ER-4 team, the advisors were able to borrow several five-ton trucks and one front-end loader to fill them. There were no operators available to run any of the machinery, so the ruthless, intrepid advisors began a "trial and error" fill dirt operation, that would have put "Conte" out of business in a week. Anyway, two weeks and 184 truckloads later (overlooking hours of exasperation at the controls of the front-end loader, or back and vocal strain when trucks were "unprofessionally" backed too far into "mini-lake" and had to be "push-pulled" out), the base level was nearly workable. However, continuous rains along with the rising water table, postponed any substantial achievements until early December '72 when the earth finally dried up and initial work began on the installation of the TRD-23.

While operations were running as smoothly as could be expected at "mini-lake", 500 meters to the Northwest was another facet of the MRDF project. This was the location of the obsolete AN/TRD-4 site where some of the equipment for the "mini-lake" had been stored. The removal of this equipment left only the hut, connecting cables and antennas. By order of the Commander of Can Tho airfield, a different section of perimeter grass was burned each month. As fate would have it, the date for burning grass in the area of the TRD-4 site coincided with the operation at "mini-lake" and no advisors were available to monitor the burning. G.I.'s from the airfield command trudged out early one morning to begin their detail. With gasoline cans and blow torches, they began what was supposed to be a small, controlled, well supervised grass fire. All went well for the first hour or so. Personnel were strategically placed armed with shovels and rakes, just in case something should happen. An undetected slight change of wind (in volicity and direction), began to move the fire towards the AN/TRD-4 hut and its many antenna cables. Before

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

anyone realized what was happening, the highly inflammable cables began to burn and spread towards the remaining antennas. This probably could have been stopped with a minimum of effort, if there had not been a war in progress. ARVN helicopters returning from a sweep and destroy mission, flying low over the airfield, fanned the flames in every direction at once, creating pandemonium and mass chaos. Before the fire could be brought under control, approximately \$1,500.00 worth of cable, connectors and antennas had been destroyed.

Meanwhile, back at "mini-lake", to insure that future rains would not destroy the equipment installed for the TRD-23, everything was elevated 1 foot. This was accomplished by pouring concrete antenna pedestals (12" high) for each of the 26 antennas and two (12" thick) 12X18' slabs to support the generators and the TRD hut. All this was completed in three weeks, with most of the time being consumed scrounging cement and lumber for forms. Before any antennas could be placed on their respective pedestals, four perimeter poles (each 40' high) had to be erected in each of the four corners of the antenna array, with aircraft warning lights fixed to the top of each one. (This was necessary because "mini-lake"/TRD-23 site was only 200 feet from the end of the Can Tho airfield runway). As soon as the poles were in place the lights had to be operational; thus another project was temporarily halted until a power source could be found. The only generator in the area was owned by the Pacific Architects and Engineers (PA&E/-AKA- promises, alibi's and excuses); so advisors approached them and obtained permission to use their generator. Yet another delay of three weeks was incurred because PA&E had another requirement to supply power for the joint military commission (JMC) and the international commission for control and supervision (ICCS) peace-keeping forces while they were at Can Tho airfield. The delay came as a blessing. Checking their cable supply, the advisors discovered a shortage and the generator in question was approximately 1/4 of a mile away. After securing additional cable, the day finally came when the power was available. When the poles went up, the electrical cable was laid 1/4 of a mile to the generator, the aircraft warning lights were working and now the final installation of antennas could begin. Not two hours later, a Vietnamese garbage truck, making its daily run through the airfield, veered off the road, cut the electric cable just laid, and fell two of the 40 foot poles supporting the aircraft warning lights. Had the advisors not been pillars of virtue and possessed of great fortitude, this would have discouraged them. But, being ruthless, intrepid types, they had the cable spliced and the poles back in place in a matter of hours.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Finally, on St. Valentine's Day 1973, the metamorphosis of "mini-lake" was a reality and Can Tho's AN/TRD-23 MRDF site became operational. ARVN personnel, however, were not familiar with even the most basic maintenance procedures to support the site. Any outages that occurred were normally extended until TDY personnel from Saigon could diagnose the malfunction and acquire the necessary parts.

Inadequate maintenance capabilities not only plagued the MRDF site, but all facets of operations--vehicles, generators, air conditioners, commo/signal-equipment, etc. Since CTC was only permitted to perform first echelon maintenance, repairmen assigned received only limited training as opposed to the extensive schooling afforded their U.S. predecessors. As a result of limitations, any equipment malfunctions usually had an extended adverse effect on the entire operation.

As at any other field station, Can Tho's nucleus was the communications center (C.C.). Without this equipment running smoothly, the station was cut-off from the rest of the intelligence community.

Prior to January '73, W33's (intercept designator for CTC) C.C. experienced many maintenance problems. Because of cramped working conditions, maintenance personnel could not perform daily preventive maintenance (PM), which resulted in many operational hours lost. Recognizing the "cracker box" problem, advisors suggested to higher headquarters (Unit 15 - Saigon Center), that the C.C. at Can Tho be relocated to the area vacated by the U.S.C.C. This move would facilitate the following: first, daily PM could be performed, thereby eliminating approximately 50% of equipment down-time; second, the addition of three new circuits (two with Saigon/one with the proposed 44th Support Platoon) could be accommodated; third, a significant amount of circuitry and equipment was left by the U.S. communications people which would simplify the transition; fourth, the proposed area provided ample space to house all C.C. equipment and would also allow for further expansion should the need arise; and finally, the new area had the much needed direct air conditioning ducts to aid in keeping the equipment cool and operating. With Saigon's concurrence, the move was made and the C.C. began to run smoothly.

For any operations to run smoothly, constant supervision and guidance are necessary; therefore, every month the senior advisor accompanied the CO/CTC on his inspection tour to the

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

three subordinate ASTD's. These trips provided an on the spot review of equipment, personnel, problems at hand, and any foreseeable problems could be discussed.

Transportation was always the fastest, best mechanically tuned jeep available at CTC, while the ARVN driver was a conglomerate of Andy Granatelli, Richard Petty, Bobby Unser and Steve McQueen. This combination of driver and jeep was needed most on trips to the 7th ASTD located in Dinh Tyong Province. To reach the 7th from My Tho City, a spine-tingling drive along "ambush alley" (a stretch of road approximately 1000 meters long, flanked by thick jungle on both sides) was necessary. This was where jeep, driver and all occupants hoped for a new speed record on each and every trip.

These monthly sojourns into the VC/NVA occupied suburbs of the Mekong Delta, also allowed for sampling of the local culinary/gastronomical delights offered at the many roadside stands. These stands are known by many pseudonyms: "Ba muoi ba" stands (named after the Vietnamese Bier "33"), "Hepatitis Stands" (named after "post dinner complications"), and more commonly known to all as "the local Howard Johnsons". Inevitably upon their return to Can Tho, the ruthless, intrepid advisors proceeded posthaste (usually with a gait reminiscent to that of the "Green Apple Quick Step"), to the dispensary for a small white envelope humorously marked "Stop Gap", or "Cement Pills, for internal use only".

The successful transition from U.S. to ARVN COMINT operations has been evaluated and found satisfactory. The only unanimous regret, reflected by both ARVN and U.S. personnel involved, is that the VIM Program didn't begin earlier. Naturally, there is always room for improvement; but, keeping in mind the "newness" of the Vietnamese in the COMINT business, much credit must be given for their many accomplishments in such a short period of time. The advisors at Can Tho Center feel that the desire of the Vietnamese to constantly better the quality of their COMINT product will continue and enhance the overall Vietnamese Intelligence effort.

NOTE: The preceding article only high-lighted some of the achievements and humor associated with the Vietnamization Improvement and Modernization Program in IV Corps. To discuss the numerous anomalies and corrective actions that occurred on a daily basis would be cumbersome and would detract from the continuity of events. In reality, these daily occurrences often had the characteristics of the aimless wanderings of an odyssey and the futility of attacking windmills.

~~TOP SECRET UMBRA~~



CHRISTMAS AT THE SCHOOL

by Morris L. Ferguson, B43

On the first day of Christmas my Instructor gave to me:
A Wired Rotor in a maze of three.

On the second day of Christmas my Instructor gave to me:
Two Endplates steckering, and a Wired Rotor in a maze
of three.

On the third day of Christmas my Instructor gave to me:
Three Lobsters rolling, two Endplates steckering,
and a Wired Rotor in a maze of three.

On the fourth day of Christmas my Instructor gave to me:
Four Stem-Top Mushrooms, three Lobsters rolling, two
Endplates steckering, and a Wired Rotor in a maze of
three.

On the fifth day of Christmas my Instructor gave to me:
Five Stepping Wheels, four Stem-Top Mushrooms, three
Lobsters rolling, two Endplates steckering, and a
Wired Rotor in a maze of three.

On the sixth day of Christmas my Instructor gave to me:
Six Shrimp a-shrimping, five Stepping Wheels, four
Stem-Top Mushrooms, three Lobsters rolling, two
Endplates steckering, and a Wired Rotor in a maze
of three.

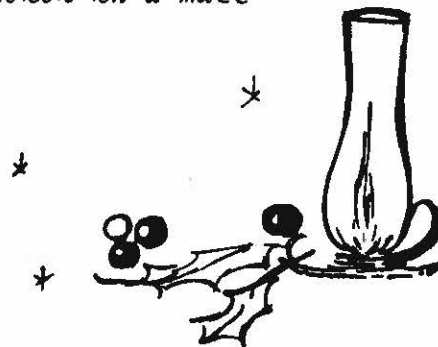
On the seventh day of Christmas my Instructor gave to me:
Seven Parallel Wires, six Shrimp a-shrimping, five
Stepping Wheels, four Stem-Top Mushrooms, three
Lobsters rolling, two Endplates steckering, and a
Wired Rotor in a maze of three.

On the eighth day of Christmas my Instructor gave to me:
Eight F's a-stripping, seven Parallel Wires, six
Shrimp a-shrimping, five Stepping Wheels, four
Stem-Top Mushrooms, three Lobsters rolling, two
Endplates steckering, and a Wired Rotor in a maze
of three.

*

*

*



*

*

On the ninth day of Christmas my Instructor gave to me:
Nine Inverse Rod Squares, eight F's a-stripping,
seven Parallel Wires, six Shrimp a-shrimping,
five Stepping Wheels, four Stem-Top Mushrooms,
three Lobsters rolling, two Endplates steckering,
and a Wired Rotor in a maze of three.

On the tenth day of Christmas my Instructor gave to me:
Ten Diagonals running, nine Inverse Rod Squares,
eight F's a-stripping, seven Parallel Wires, six
Shrimp a-shrimping, five Stepping Wheels. Four
Stem-Top Mushrooms, three Lobsters rolling, two
endplates steckering, and a Wired Rotor in a maze
of three.



On the eleventh day of Christmas my Instructor gave to me:
Eleven Reflectors reciprocating, ten Diagonals
running, nine Inverse Rod Squares, eight F's
a-stripping, seven Parallel Wires, Six Shrimp
a-shrimping, five Stepping Wheels. Four Stem-Top
Mushrooms, three Lobsters rolling, two endplates
steckering, and a Wired Rotor in a maze of three.

On the twelfth day of Christmas my Instructor gave to me:
Twelve K's a-boxing, eleven Reflectors reciprocating,
ten Diagonals running, nine Inverse Rod Squares,
eight F's a-stripping, seven Parallel Wires, six
Shrimp a-shrimping, five Stepping Wheels. Four
Stem-Top Mushrooms, three Lobsters rolling, two
Endplates steckering, and a Wired Rotor in a maze
of three.



x

*

~~TOP SECRET UMBRA~~

TIME TO LOOK AT PEOPLE

By Tom Glenn, B61

Many, perhaps most, of the organizations within B Group have been facing tough times lately. Billet cuts, some of Herculean proportions, and the resulting excess lists; moves from job to job; lack of promotions; and rife rumors of RIFS or worse--all have worked against us. The Director has asked us ("People Concerns," 12 October 1973) to give "compassionate, intelligent attention to the concerns of our people as a most important requirement of our management." It's high time we did.

According to the latest estimates I have been able to find (and these are hearsay--I cannot confirm them), NSA now spends more than two-thirds of its budget on salary; given the radically changing budget-salary ratio in years to come, we will soon reach three quarters. It would make eminently good sense, therefore, if we spent a commensurate amount of management time concerning ourselves with doing the right things to make our people effective and efficient. From my observations, I am convinced we do not, and the effects will come home to roost sooner rather than later.

Our stress in personnel management has consistently been on the external rules of operation vice common sense about what makes people work effectively. We spend enormous energy, for example, considering whether people fit the billet structure instead of whether the billet structure fits the people. We concern ourselves with numbers of people assigned in various categories instead of addressing who it is we need to get the job done. We have, in effect, created a myth world of personnel rules prodigious in their complete divorce from operational needs, and more important, from common sense approach to the concerns of people.

The impact on people of these rules has been less in the past than it is now, partly because we have never before applied them relentlessly and partly because the abundance of our budget in the past gave us slack and flexibility we no longer have. We have now learned, if nothing else, the disastrous effects on morale and productivity that unquestioning execution of personnel rules can cause. The problem is that we continue to do it anyway.

I am at a loss to understand why we do this. It may be partly because conventional wisdom dichotomizes concerns for productivity and concern for people (e.g., Blake-Mouton's management grid). But it takes little experience to stumble on the blunt truth

~~TOP SECRET UMBRA~~

that in people organizations, people are the source of productivity. Only a feeble effort of the mind is required to carry the logic further--that people involved in problem solving or other creative endeavors (such as net reconstruction, code recovery, cryptanalysis, translation, report writing) do much better when they are happy than when they are not. In short, concern for productivity means concern for people so long as any initiative whatever is required.

But maybe we are really not concerned with productivity at all. As deranged as that sounds, I suspect that many an organization in B Group has not consciously addressed what it considers to be its output (its product, if you like) and how to measure it.

The inescapable conclusion of all this is that we in B Group must direct our foremost efforts towards our people vice things (collection gadgets, machine programs, telephone fixtures and typewriters). Unless, of course, we are really not concerned with productivity.

As must be obvious to the reader, I am abashed and puzzled by what I think I see going on. I'd be pleased to know the readers' thoughts.

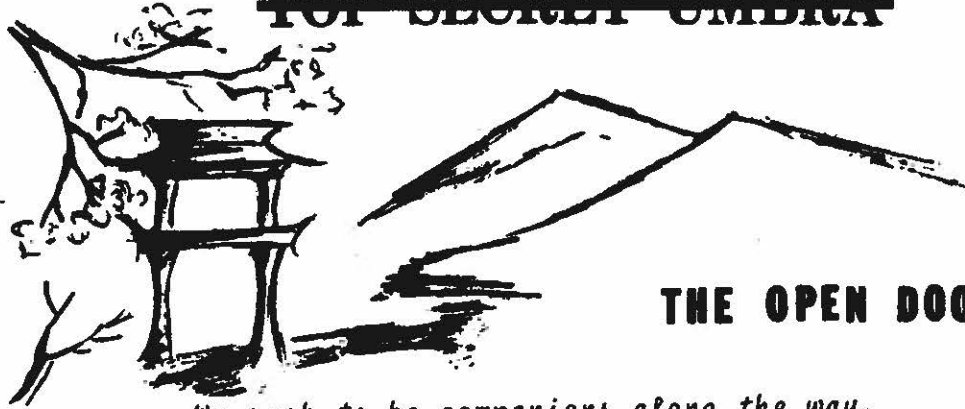
* * *

*"If those who are excellent
find no preferment,
The people will cease
to contend for promotion."*

---Lao Tzu

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



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

ARE YOU USING COMPUTERS?

by Dr. Walter Jacobs

Does fear of the computer discourage you from using it to help you in your work? If so, you may be hurting your chances for advancement. You can accomplish much more when you properly use the computer than you can without it.

A person who distrusts computers may be subconsciously afraid the computer might take away his job. True, computers today are doing many things that, ten or twenty years ago, had to be done by people. However, these things are tasks that demand no judgment, and call for repetitive operations following consistent rules. Unless a job is challenging - unless it continually draws on the imagination, initiative and intelligence of the one doing it - it may be performed carelessly, inefficiently, and with limited attention. In that case it may be true that a computer can do it better.

In most jobs, however, a substantial amount of time is spent on routine and repetitious work. If much of this work can be turned over to the computer, more time and attention can be given to those aspects of the job that require experience and expertise. The work becomes more stimulating, and the product improves in quality and quantity.

When you begin to organize your work to make use of the computer, the fresh look you take at what you are doing can bring unexpected benefits. New and better approaches you may have overlooked could surface. A case in point happened in the field.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

of medical diagnosis and its implications for Agency professionals should be clear.

A project was set up in New York City, some years ago, to develop a computer procedure to do differential diagnosis of coronary heart disease; two expert heart specialists were selected to work on the project. There are 22 varieties of ailments involving the coronary arteries and their symptoms are often so similar that even specialists cannot be sure which is present; only surgery or - worse yet! - an autopsy reveals the specific trouble. In a set of actual cases assembled as data to be used in the project, the specialists were able to make an exact diagnosis in only 72 percent of the cases.

These specialists, working with an experienced systems analyst, developed a computer program that could reach a diagnosis from the type of information provided. Using the same data, the first program gave correct results in about half the cases. Applying continued effort over a period of two years, the specialists improved the procedure to the point where its score, on a new set of test cases, rose to about 70 percent. But the specialists themselves, with the sharpened understanding they had gained in the project, were nearly 90 percent correct on these new cases.

Of course, the computer procedure could not be relied on to replace a physician in doing diagnosis. It does seem clear, however, that the doctor could improve his diagnoses with the help of the program. Especially when it incorporates the experience and technique of the best practitioners, its contribution should enhance his own decisions, except where he simply accepts the computer results in an uncritical way. Perhaps a doctor who would do that ought to be replaced by the computer!

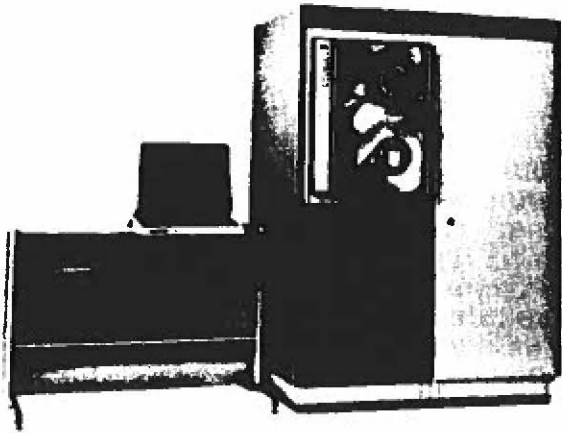
Learn about the computer programs that are available in your field. They may help you do a better job. Use them with understanding and judgment. Make improvements to the procedures where your knowledge allows you to do so. Your own career, as well as the Agency's work, will benefit.

* * * *

~~TOP SECRET UMBRA~~

MINNIE'S MINI

by Minnie M. Kenny



It seems like ages ago when it all began. We were still at FANX and had just experienced the nine hundred and ninety-ninth power outage. No COPE, no RYE, no 6700, no NOTHING!!! To top it all off, it wasn't even raining. Now what kind of Providence is that?

We came up with an idea: why not hang a tape drive on that modified PDP-8 called the COPE terminal, boosting its memory by 4K, and declare our independence from Central Control? No way!! We got bottled up in channels and buried under paperwork.

That's when I began dreaming of desk-top terminals for C/A applications. Can't you imagine a user-controlled system of minicomputers, say one master and three slaves with an interchangeable hierarchy (to eliminate service interruption when there's a malfunction), and a terminal on each analyst's desk? Why you'd hardly need cross-section paper and pencils!

One day I stumbled across several idle CRTs. I was nosing around down in C at the time. I HAD to have them. Hooked up to one of the general processors, they'd make an adequate substitute for my dream system. I lost out again. I could pirate the terminals but I couldn't "bootleg" the hook-ups.

About this time, R came on the scene touting minicomputers with blisters. They were developing interactive C/A applications. And they wooed me with the promise of the realization of my dream. We formed a committee which formed a study group which formed into teams which inspected C/A processes in B. The results are discussed in the following article, but . . . I STILL WANT A MINI.

B NEEDS ITS OWN COMPUTER

by William P. Stivers, H11

Recently R conducted a 5 month study called ALBRECHT to determine whether an interactive computer need existed in B Group for the analysis of low/middle grade cryptosystems. A five member study group composed of one member each from R111, R113, R252, R313 and a CA intern with experience in B1 determined that such a need did exist. The study group found that with an interactive computer many of the B target systems could be solved more efficiently and the time and versatility gained could be aimed at solving other B target systems. The formal ALBRECHT STUDY report explains how the study was conducted and describes a computer system that would provide the interactive capability needed in B. This article is a review of the main sections of the ALBRECHT report and is especially intended for those who may not read the formal report.

The ALBRECHT study began with visits to analysts in B1 to see the types of CA problems being worked and the techniques used in attacking the problem. ALBRECHT visits focused on B1 because earlier tasking, prior to the reorganization and physical moves, had emphasized looking at that organization. The types of CA problems being worked included diagnosis of unknown systems, recovery of parameters of diagnosed systems, and decryption.

In the first type of problem, diagnosis, an interactive system would facilitate the processes by instantaneously providing STET statistics while at the same time offering versatility to rapidly manipulate the data for other tests. For instance, if the tests indicated significant scores for a particular width, the analyst could quickly and simply display the message on that width. If null groups were suspected they could be edited out of the message with a few simple statements. Each analyst could develop, for his own data, countless displays and tests, all of which would be rapid in execution and yet relatively simple in construction.

The second class of problems, parameter recovery, is especially suitable for attack by an interactive computer. Here, where the "modus operandi" is trial and error testing of assumed parameters, the interactive system would provide a rapid means for testing these assumptions. For instance, an analyst working a problem diagnosed as transposition; but with an unknown width and key, could repeatedly display the text on a

~~TOP SECRET UMBRA~~

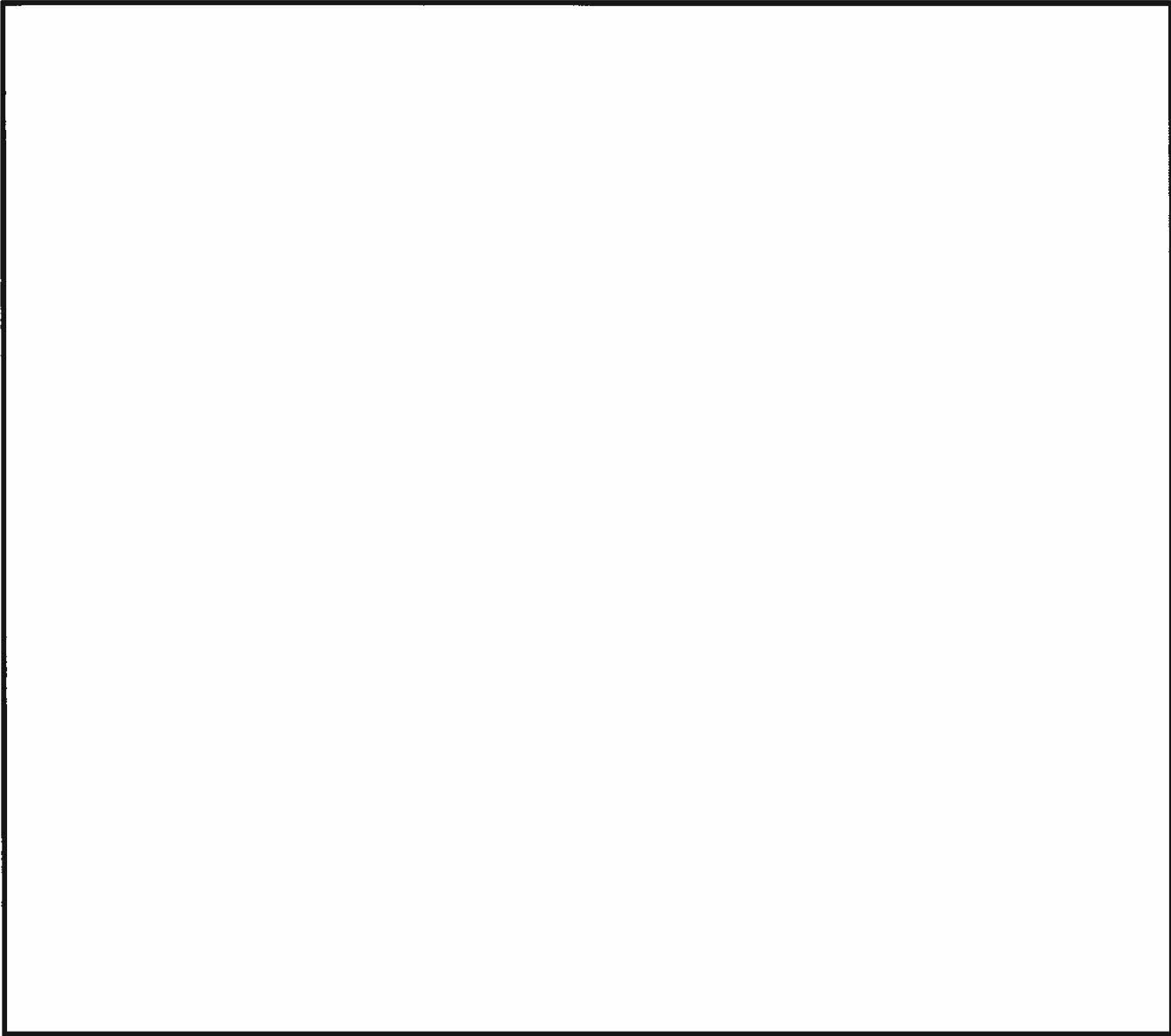
scope according to assumed widths and keys. After each display the analyst would base his next assumption on observed digraphic properties and other latent patterns, until plaintext started forming. In a chart system where a particular cipher group had several possible meanings, the analyst could rapidly test each assumed meaning to determine which one was most likely correct. Numerous other situations involving trial and error procedures with human intervention for decision making are done most efficiently on an interactive system.

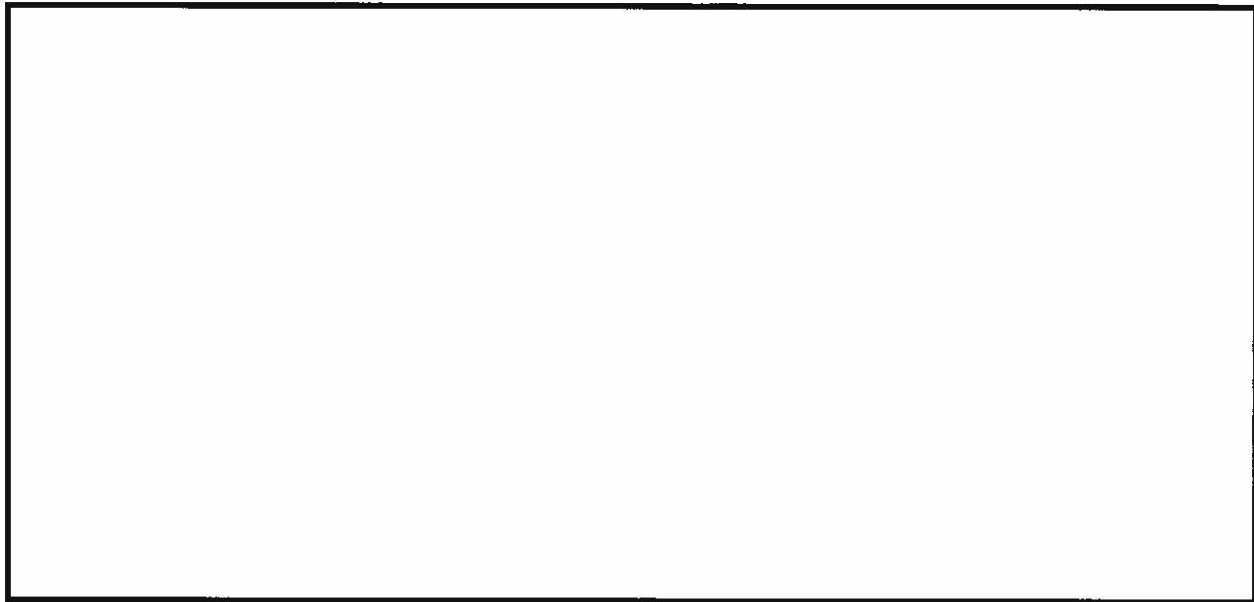
The third class of problems, decryption, is not a prime candidate for attack by an interactive computer. If all the parameters are known and the decryption process can be put into a clearly defined algorithm, the problem is better solved on a compiler system without interaction. If some of the parameters are sketchy, however, or if they are subject to frequent change, the interactive system could again be a useful tool.

During the visits to Bl, ALBRECHT also observed some non-cryptanalytic problems that confront the analysts on a daily basis. For instance the analysts have a problem of storing message hard copies, data paper tapes, data and program cards, cipher and code charts, and other miscellaneous program runs. Most of the storage is in desks, cabinets, and boxes where retrieval after any period of time longer than a week becomes cumbersome. With an interactive computer having large file capability, the analyst could store much of the above materials in files, and quick retrieval would be an elementary procedure. Editing was also cumbersome when data had already been punched on paper tapes or cards. Often, if the analyst wanted to add or delete characters or non-textual groups the data had to be repunched. In an interactive computer system, editing chores such as changing, adding, or deleting characters and groups are simple matter-of-fact operations. Another problem the analysts faced was the incompatibility of the machine aids being used. There was a RYE terminal with paper tape input, a 360 COPE terminal with card input, and a Burroughs outstation which also had card input but with special character punches different from those of the COPE terminal. A file-structured interactive system where programs and message texts could be stored in files would eliminate the incompatibility problem. The analyst could do all the work at one terminal using files which had been created from desired peripheral input devices.

~~TOP SECRET UMBRA~~

After visiting the analysts in B1, members of ALBRECHT wrote APL programs for some of the CA problems they had observed. The particular problems chosen were not the only ones suitable for interactive attack, nor were they considered the best candidates for interaction. They were simply chosen out of interest. The study group used APL to program the problem because it is a truly interactive language and facilities for its use were convenient.





In each of the demonstration problems programmed by ALBRECHT, the advantages gained in continual accuracy and time saved were sizeable. The human intervention for decision making, which usually took the place of a branch that could not have been canned in a neatly defined algorithm, was the predominant asset of the APL program.

Along with the visits to B and the demonstration programs, the ALBRECHT study continued with technical demonstrations, briefings and directed research. Then, prior to stating the actual system recommendations, the study group made some general observations, the main area of which dealt with programming languages. Three languages, APL, FORTRAN, and BETA, were mentioned though ALBRECHT did not experiment with FORTRAN and BETA; FORTRAN because it was not felt necessary and BETA because it would have delayed the study to learn it, resources were not readily available, and in no way was it the intention of the study to evaluate BETA.

APL is a truly interactive language that permits human intervention for decision making and redirection of the program. Its mathematically oriented symbolism allows experienced programmers to write concise statements to perform the desired analysis. The ease of character handling and the ease of array-structured data manipulation make APL attractive to the CA analyst programmer. APL is ideally suited for short lived problems where the advantage of decreased programming time outweighs the consideration of CPU

~~TOP SECRET UMBRA~~

time. This is important in B Group where ALBRECHT has observed that some of the demonstration problems programmed by the study group have already died. APL is also well suited as a test vehicle for new ideas or problems.

FORTRAN is a well known and widely used compiler language. Versions of FORTRAN, more or less compatible with each other, exist on all computer systems. Being a compiler it produces efficient code and is well adapted for longer running jobs. FORTRAN certainly should be on any NSA system.

BETA is an NSA developed and maintained compiler language. It is oriented toward character and bit stream manipulation and cryptologic processes. Since ALBRECHT never experimented with BETA it cannot comment on BETA's overall desirability or how easy it is to use or learn.

At the conclusion of the 5 months of study ALBRECHT made recommendations for a system to meet B's interactive needs. ALBRECHT suggested that B Group be given definite access to a medium-to-large general purpose computer. The system should be file-oriented time sharing with a large file storage capability. The file storage capability must be large (perhaps as much as 32 million bits/user) since most of the data handling problem would be eliminated if all current and many past messages and analyst's programs could be stored in files.

The ability to create, edit and peruse the files from the terminal is deemed a necessity for the proposed system. The files must be easily spliced together and they must be easily linked as input to any job executed in any mode or written in any system language. The linked files may be submitted at the terminal as either a time-sharing job (immediate run) or as a batch or background job.

The essential programming languages for the system are FORTRAN, APL and assembly language.

Batch mode processing should be initiated at the terminal using files. Also, the analyst should be allowed to decide by inspecting an output file whether the output should be sent to the line printer.

The analyst should have ready access to the terminals and most of the terminals should be of the CRT (cathode ray tube) type with identical keyboard and character sets. With a file oriented system using CRT's, much of the hard copy output can

~~TOP SECRET UMBRA~~

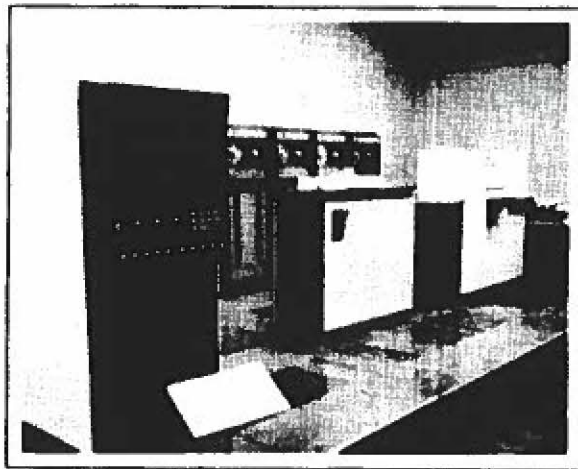
~~TOP SECRET UMBRA~~

be suppressed, but it is still essential to have hard copy output readily available. A system line printer is essential and one or more typewriter terminals and/or device(s) that reproduce the CRT screen by photo-copy could be provided.

All character data throughout the system, whether in core, in file storage, or in passing from or to the peripherals or terminals should be in compatible form.

ALBRECHT' also suggests that B Group secure several 370 APL terminals as an intermediate action while pursuing the above proposed system. The 370 APL terminal is a powerful analytical tool and its introduction into B Group would significantly enhance B's cryptanalytic effort.

* * * *



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



~~S SPOKE~~

FM DIRNSA

TO USM-7

~~S E C R E T SPOKE~~

+B65-1248-73

CAMBODIAN PROCESSING

YOUR 260730Z NOV 73

1. THE FRENCH ABBREVIATION GRUNC EXPANDS QTE GOUVERNEMENT ROYAL D'UNITE NATIONALE DU CAMBODGE UNQTE QTE GRUNK UNQTE EXPANDS GOVERNEMENT ROYAL D'UNITE NATIONALE DU KAMPUCHEA UNQTE. BOTH XLATE QTE ROYAL GOVERNMENT OF THE NATIONAL UNION OF CAMBODIA UNQTE. QTE RGNUC UNQTE IS THE ENGLISH EQUIVALENT OF GRUNC/GRUNK. WHEN ABBREVIATION QTE GRUNC UNQTE OR QTE GRUNK UNQTE IS OBSERVED IN A MSG. PLS USE APPROPRIATE ABBREVIATION IN XLATION AND FOOTNOTE QTE ROYAL GOVERNMENT OF THE NATIONAL UNION OF CAMBODIA UNQTE. GRUNC OR GRUNK ARE THE ACCEPTED ABBREVIATIONS FOR CAMBODIAN PRODUCT.

XGDS 2

REVIEWED BY N. P. MOORE, D/CH, B651/MR. LEE, B65

CONCUR B609, MR. JAMIESON

B09, MR. CHASE

B, B6, B65, B7, G923, ASALNGP

W. R. NIEDERHAUSER, B6512, 7196S GEOFFREY C. WOOD B65 7178S

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

[REDACTED]

by Russ Myers, B65

Some years ago it was discovered that the majority of code reconstruction problems could be serviced by a general-purpose package of programs. This discovery led to the development of the Bookbreaker's Package which, in its Version 1, fulfills the analyst's minimum initial machine run requirements. The package, designed in C53 (now G46) in close cooperation with bookbreakers from G, parallels Swift's *Standard and Techniques of Code Reconstruction*. Its Version 1 provides a standard bookbreaker's index, a beginnings sort, an endings sort, a decoded vertical message print, a message header log, and listings of all recovered code groups residing in the code meaning file in inverse frequency order, decode order, line-page order, and encode order. There also exists a Version 2 which permits the updating of message and meaning files and a Version 3 which provides for a Decoded Bookbreaker's Index (the meaning for a code group, when available in the meaning file, is substituted for all occurrences of that code group in indexed text).

A more recent programming effort by Mr. Bill Davis of B209 for bookbreakers of Chinese-language codes, produced the Text Index procedure.

[REDACTED]

At the direction of Ms. Minnie Kenny, B4 TDLA, a procedure has now been developed to combine the best features of both the Text Index procedure and Version 1 of the Bookbreaker's Package. Mr. Mike Fresty, formerly a Data Systems Intern in B65 and now permanently assigned to G46, was selected by Ms. Kenny to provide the IBM370 JCL and POGOL language changes necessary to link the two procedures. Although the procedure was originally prepared to assist B21 bookbreakers, it can be used with little modification, for any tetronomic code whose messages are resident in an AG-22/STRUM data base.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Essentially, the new procedure has all features of Text Index up to the creation of horizontal message prints. These are stored on an intermediate disk file in a format compatible to that required by the Bookbreaker's Package. A call is then made to the Bookbreaker's Package to produce all Version 1 outputs.

The procedure has been setup to run via COPE RJE; however, it should be noted that when a significant volume of data is involved, the procedure should be run at the IBM370 mainframe. In its present form, the procedure will not allow the user to selectively produce output options of the Version 1 Bookbreaker's Package; however, relatively minor changes i.e., insertion of dummy cards, could accommodate such a requirement. Additionally, the SPECOL language selection criteria composed by the user must be such that he can assure a run against a homogeneous set of data. The most readily available retrieval fields are date, case notation, and cryptosystem title. For full effectiveness, when discriminating among cryptosystems, the user should assure that either a "front-end" weighting routine is used or that the specific cryptosystem title is inserted in the appropriate field through data base file maintenance.

For additional information on this new procedure, contact Ms. Kenny of the B4 Technical Directorate, room 7A144 (5414s).

* * * *

TD QUOTES -

"It seems that 2/3 of the people we hire in this Agency are to throw roadblocks in the way of progress."

--- G. S.

~~TOP SECRET UMBRA~~



----SEEK THE BIZARRE SOLUTION -

Are you thinking about better ways to do your job?

Are you frustrated because your good idea would require too many others to change their ways?

Are you tired of doing it by hand when the machine could and should do it faster?

The Technical Directors want your ideas on how B can work together to do the job better. No suggestion for improvement is too outlandish or bizarre to consider. Call us:

LANGUAGE	- 5414s
CRYPTANALYSIS	- 5978s
TRAFFIC ANALYSIS	- 5978s
AUTOMATED SYSTEMS	- 5007s

----ANNOUNCEMENTS OF CMI AND CLA ESSAY CONTESTS. CMI ESSAY CONTEST - RULES SLIGHTLY REVISED.

Papers are now being accepted for the 15th annual CMI Essay Contest. All entries should be submitted to Miss Judy Bennett, G4, 3A114, extension 3109, no later than March 29. Type-written manuscripts are preferred, and three copies should

be submitted. Necessary diagrams or drawings should be included.

The purpose of the contest is to recognize professional accomplishment and to foster documentation of new and/or important ideas in cryptomathematics. At the annual CMI banquet, prizes of \$100, \$50 and \$25 will be awarded in accordance with the recommendations of the panel of judges. All entries submitted will be considered for publication in the NSA *Technical Journal*.

All NSA employees, including non-members of the CMI, are eligible to enter the contest. In addition, any member of the CMI who is not an NSA employee may also enter. Papers may be submitted on behalf of their authors, providing the author is eligible and consents.

Any writing on cryptology or a significantly related topic may be entered. Security classifications are permissible. Compartmented papers will not be accepted, but any techniques or ideas originating in compartmented

problems may be reduced to a noncompartmented level. All NSA *Technical Journal* articles of the current contest year will be automatically considered as entries.

Papers published outside NSA are also acceptable as entries. Authors may wish to perform some revision or addition to make the relevance of the subject to cryptology or related topic more explicit. If such relevance to cryptology is not or cannot be supplied, judges may use its absence as a primary reason for eliminating the paper from further consideration.

The CMI will select the panel of judges whose names will be announced when all papers have been submitted. Judges of the contest are not eligible to enter. Criteria for judging are: a) Relevance to mathematics and cryptology, b) Significance of the content to Agency operations, c) Interest of the paper to Agency professionals, d) Quality of the writing.

CLA ESSAY CONTEST

The eighth annual essay contest of the NSA Cryptolinguistic Association is now open, and papers will be accepted until March 15th, 1974. The purpose of the contest is to encourage writing on topics concerning the application of linguistic knowledge to the solution of Agency-related problems so that organized information can be

disseminated among professionals in this field. At the spring meeting of the CLA prizes of \$100, \$50 and \$25 will be awarded in accordance with the recommendations of the panel of judges. All entries submitted will be considered for publication in the NSA *Technical Journal*.

Any NSA employee, regardless of his membership in the CLA, is eligible to enter the contest. In addition, any member of the CLA who is not an NSA employee may enter. Papers may be submitted by others on behalf of their authors, provided the author is eligible and consents. Judges, however, are not eligible.

Any writing on cryptology or a significantly related topic may be entered. Security classifications up to and including TSC are permissible, but techniques and ideas originating in compartmented problems must be reduced to a noncompartmented level. All NSA *Technical Journal* articles of the current contest year will be automatically considered as entries unless they have been considered in a previous contest.

Typewritten manuscripts are preferred, and three copies should be submitted. Necessary diagrams or drawings in finished form should be included.

Papers should be submitted to Mrs. Constance H. Grisard, G94, Room 2S010, Operations Building #1, extension 4812s.

The CLA will select a panel of judges whose names will be announced when all the papers are in. Criteria for judging are:

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

Papers published elsewhere (outside NSA or in the NSA *Technical Journal*) are acceptable as entries. Authors may wish to perform some revision or addition to make the relevance of the subject to cryptology or related topic quite explicit; it may not have been necessary or possible to do so in the original publication. References to the areas where the problem occurs or where the ideas can be applied may well be incorporated into contest submissions so that judges and other readers do not have to supply this pertinent information. If such relevance to cryptology is not or cannot be supplied, judges may use its absence as a primary reason for eliminating the paper from further consideration.

Compartmented papers will not be accepted, and any work which because of its length would not be suitable for publication in the NSA *Technical Journal* will not be accepted.

----Have you tried CANDE??
It's out of sight!!
You should see what Russ Myers and cohorts in B65 are doing in the way of interactive C/A applications. Why don't you call him and get a demonstration? That's 3447s.

----LANGUAGE TESTING SYMPOSIUM
13, 14 March 1974
(Immediately preceding the
Georgetown Roundtable)
New South Faculty Lounge
Georgetown University
Washington, D. C.

Sponsored by member of the United States Government Interagency Language Roundtable (Foreign Service Institute of the Department of Defense, Office of Education of the Department of Health, Education and Welfare, Central Intelligence Agency, National Security Agency), the Center for Applied Linguistics and the Commission on Tests and Testing of the International Association of Applied Linguistics (AILA).

Purpose: To explore problem areas of testing language proficiency as it relates to the use of foreign languages on the job. Among the topics of discussion will be: the oral interview test, remote testing of speaking proficiency, cloze testing, reduced redundancy testing, criterion-referenced testing and subjective vs. objective language

~~TOP SECRET UMBRA~~

tests. During each of the four sessions of the symposium two or three presentations will be made. Each presentation will be discussed in detail by a panel of invited participants.

The public is cordially invited. If you would be interested in attending, please fill out the registration form and return it by 22 February 1974. There is no charge for registration. A complete program will be sent by 1 March.

All arrangements for lodging and meals will be the responsibility of each individual. Information about hotels and motels in the Georgetown area will be sent on request. Registration form should include Name, Address, Country, and Institution. Please indicate if you need hotel information or further information about the Georgetown Roundtable. Return completed forms to:
LANGUAGE TESTING SYMPOSIUM
P.O. Box 9569
Rosslyn Station
Arlington, Va. 22209

----Did you know that copies of Communist Propaganda Highlights prepared by the Psychological Warfare Research & Intelligence Division are now available in the B Language Media Center, Room 3S078? See George Sing, ext. 5309s/5310s.

----Future CMI Lectures:

7 March 1974 - Mr. E.

Speigelthal, Rlll,
"Representation of
Integers - A Linguistic
Problem."

4 April 1974 - Prof. S.

Kullback, George Washington
University, "Contingency
Table Analysis."

2 May 1974 - Dr. N. Zierler,

IDA, "A Computational
Problem in Finite Fields."

17 May 1974 - Prof. J. Tukey,

Princeton; Bell Telephone
Lab, Topic to be announced.

6 June 1974 - Mr. T. Evans,

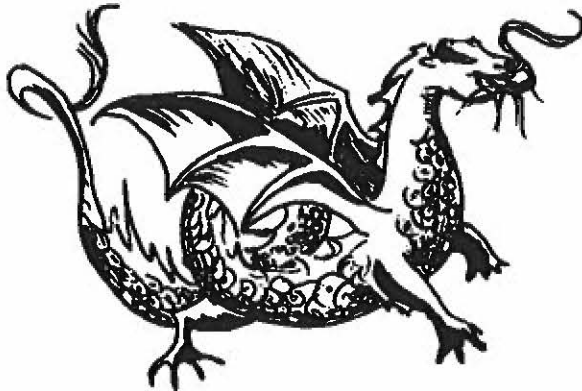
Pl, Topic to be announced.

----C announces a new programming system for the CDC 7600 and IBM 370 computers. The programming system is BETA. This is a tool expressly designed to aid analysts in solving their cryptologic problems.

Many Agency personnel are using earlier versions of BETA on IBM and BURROUGHS equipments. They find it to be extremely useful in their work. With BETA available on BURROUGHS, CDC, IBM, and soon UNIVAC computers, Agency analysts now have a variety of hardware choices to meet their programming requirements.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



ASK
THE
DRAGON
LADY

Dear Dragon Lady,

Mr. Glenn's letter of last month raises a valid point concerning insights into the organization and functions of the Central Reunification Committee gleaned from SIGINT during 1958-62. However, in contrast to Mr. Glenn's suspicion, recent plaintext Civil messages reveal that the CRC is still with us, alive and well somewhere in North Vietnam, and actively involved with South Vietnamese affairs. Ms. Kennard's basic observations concerning the role of the CRC provoked us to research its current posture. We found her equation of the CRC to CP. 40 questionable in light of recently consolidated material dating from the early 1950's to the present. We are still synthesizing a large volume of SIGINT hoping to determine the CRC's present relationship with the Lao Dong Party, COSVN, the SVNLA, NVN governmental and administrative control of liberated areas in SVN and the like.

Peter J. Melly, B614

* * * *

In the continuing discussion of the linguist's plight, the Dragon Lady offers the following in an effort to refute the oft repeated equation that a "warm body + dictionary = Linguist", and to explain the Language Analyst's constant quest for the latest, most up-to-date reference works. The thoughts were excerpted from *Word Play* (Alfred A. Knopf, publisher) by Peter Farb, an anthropological linguist, former lecturer in English at Yale University, and author of several books.

". . . In short, every language offers its speaker an array of strategies with which they can play the language game. . .

~~TOP SECRET UMBRA~~

Most people assume that a text in one language can be accurately translated into another language, so long as the translator uses a good bilingual dictionary. But that is not so. . .

Despite what most people believe, dictionaries do not give the "meanings" of words. Rather, dictionaries present "meanings" by offering a selection of synonymous words and phrases - which are themselves listed in the dictionary. The dictionary thus is a closed system in which someone interested in the meaning of a word can go around and around and end up exactly where he started, simply because words are defined in terms of other words, and these, in turn, are defined in terms of still other words. . .

The "meaning" of a word in the dictionary, therefore, is not the meaning at all. It serves merely as a reminder to a speaker WHO ALREADY KNOWS HIS LANGUAGE^{1/}, has grown up in a speech community that uses the word, and who employs the hints in the dictionary to make a guess at the meaning. . .

Finally, an adequate dictionary usually takes at least a decade to prepare (the OXFORD ENGLISH DICTIONARY required about 50 years), and by the time it has been completed it is the dictionary of a changed language, simply because the meanings of words do not stay the same from year to year."

1/ capitalization supplied

* * * * *

~~TOP SECRET UMBRA~~

SOLUTION TO SEPTEMBER'S PUZZLE:

0926 9704 1899 7956 9489 0926 2939 8303 1722 1125 1172 7567
4102 5363 7831 2397 9976 4102 1367 3630 0849 4104 2455 6859

9489 1604 4436 3281 7352 5089 7984 0184 0252 1562 1624 3281
9976 2508 0191 6651 5669 5890 4099 1455 0735 4430 1331 6651

4381 1126 1172 7567 9489 1604 4436 3281 2236 0342 1126 1387
2975 4104 2455 6859 9976 2508 0191 6651 2053 0948 4104 4357

3084 1409 2559 4813 0156 2326 0187 1126 1172 7567 9390 7352
2585 0031 5030 2429 0553 4907 2837 4104 2455 6859 9975 5669

5089 5472 0103 2851 1126 4224 0324 0252 9725 9372 1551 0019
5890 0006 0008 0681 4104 1748 1709 0735 7364 2706 0668 0110

8718 8906 7984 0184 9489 1562 1624 5472 0103 2851 1126 1624
5261 3945 4099 1455 9976 4430 1331 0006 0008 0681 4104 1331

4858 1551 0019 8718 8906 8303 3181 9390 2911 3351 8169 7771
3175 0668 0110 5261 3945 3630 6158 9975 0448 3938 5887 2398

7154 3874 9489 1326 0771 2057 8169 5455 2780 9725 9372 9489
0500 6852 9976 1730 0455 2236 5887 0001 4467 7364 2706 9976

5455 2780 1624 4858 9489 4687 1393 1539 5455 2780 9725 9372
0001 4467 1331 3175 9976 4391 2972 0659 0001 4467 7364 2706

9489 1539 5455 2780 1624 4858 9489 2236 0015 4143 5321 3084
9976 0659 0001 4467 1331 3175 9976 2053 0226 6126 3634 2585

6450 6317 1870 7352 5089 0252 2780 1624 1126 7984 0184 9390
2589 1364 2456 5669 5890 0735 4467 1331 4104 4099 1455 9975

7352 5089 0252 2780 1624 0120 1126 1604 5470 4656 9514 9489
5669 5890 0735 4467 1331 0022 4104 2508 7236 0795 7344 9976

2210 7651 3276 7761 7352 5089 2072 2780 1624 2072 1126 8718
2019 3981 6639 6665 5669 5890 3954 4467 1331 3954 4104 5261

8906 7742 3181 0157 6629 4274 9489 3276 7761 7352 5089 0252
3945 6062 6158 0637 6043 3082 9976 6639 6665 5669 5890 0735

2780 1624 1126 4670 1779 0157 6629 4274 9489 8940 0103 2210
4467 1331 4104 1395 6432 0637 6043 3082 9976 5079 0008 2019

(Continued next page)

~~TOP SECRET UMBRA~~

7651 5011 2724 2988 0426 1126 1172 4814 0157 6629 4274 9390
3981 2231 0648 4675 0830 4104 2455 3127 0637 6043 3082 9975

PLAYFAIR SQUARE

00	01	05	06	14	15	27	28	44	45
02	04	07	13	16	26	29	43	46	63
03	08	12	17	25	30	42	47	62	64
09	11	18	24	31	41	48	61	65	78
10	19	23	32	40	49	60	66	77	79
20	22	33	39	50	59	67	76	80	89
21	34	38	51	58	68	75	81	88	90
35	37	52	57	69	74	82	87	91	96
36	53	56	70	73	83	86	92	95	97
54	55	71	72	84	85	93	94	98	99

* * * *

TD QUIPS -

*"Anytime you let the shape of the
vessel determine the contents, you
ARE in trouble."*

-- H. G.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

CONTRIBUTORS

MORRIS L. (LEROY) FERGUSON, B43, came to NSA in December 1963 after a three-year tour in the Army. He worked in A5 until 1970 when he entered the Cryptanalysis Intern program. Leroy graduated from the Intern program in December 1973 as a certified cryptanalyst and was assigned to B43. He is currently attending Mr. Callimahos's CA400 class.

TOM GLENN, Chief, B61, has a total of 15 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, cryptlinguistics, intelligence analysis, and most significantly, in the management of the SIGINT reporting effort on the Vietnam war. In December 1973, Mr. Glenn received his M.A. in Government at George Washington University.

WALTER W. JACOBS retired as COMMANDANT, National Cryptologic School, in October 1969 to join the faculty of The American University. He served as Chairman, Department of Mathematics and Statistics, from June 1970 to June 1973 and is at present heading the Computer Science program at the University. Dr. Jacobs comments, "What a great place the Agency is -- an unusual group of people with outstanding ability, dedication, talents, and variety of interests -- there's nothing like it on the outside!" For the past two summers, Dr. Jacobs taught an advanced programming techniques course at NSA and hopes to teach for the Agency again this summer. After Dr. Jacobs earned his PhD in Mathematical Statistics at the George Washington University, he had Military Service during World War II in the Office of the Chief Signal Officer (OCSigO) at Arlington Hall and Bletchley Park (England). Later, he served in key civilian positions involving mathematics in the USAF, in the R&D Organization of NSA, and as Chief of the NSA Machine Organization, then C4, from 1961-1963.

RUSS MYERS, B65, joined the Agency in 1965 after serving four years with the USAFSS. Fifteen months of his Air Force tour were spent at Peshawar, Pakistan, one of the "garden spots of the world." At NSA, he spent two years in A8 as a traffic analyst and Russian linguist and then was selected for Class 10 of CV100. He moved to B1203 (now B6503) in 1968 as a

cryptanalyst. Mr. Myers was a member of Class 24 of CA-400 and was detailed for six months to B42 under the B Internal Data Systems Training Program. He holds professional certification in traffic analysis, cryptanalysis, and computer systems analysis, as well as a BA in Government and Politics from the University of Maryland. Mr. Myers is currently involved in the development and management of several data processing projects for B65 problem areas.

EDWARD A. O'CONNOR served with the Air Force Security Service after receiving a Bachelor of Arts degree from Rhode Island College in 1966. He joined NSA in May 1970 as a Traffic Analytic Technician and in 1971 he was selected for an internship by the Traffic Analysis Career Panel. Currently, Mr. O'Connor is a member of UNCOAST.

WILLIAM STIVERS has been with NSA seven years, the last two of which he has spent as a CA Intern. Prior to joining the Intern program, he was assigned to the [redacted] where he gained experience in signals analysis as well as cryptanalysis. He acquired an interest in programming as an analytical tool during Intern tours which required a programmer analyst. Bill believes in doing things the hard way and, accordingly, is attending Towson State Evening School where he is a Junior.

LEO C. STEPP, B632, joined NSA in 1965. He has been involved with the Vietnamese Communist problem almost all of his Agency life. From July 1972 to June 1973, Mr. Stepp served as the Senior U.S. COMINT Officer and Advisor to the South Vietnamese Special Security Technical Branch in MR IV (Can Tho, SVN). He is currently assigned to B632 as a member of a team responsible for [redacted]

JACK THOMAS, B44, came to NSA as a CIVOP in 1956, after a 3-year tour in the Army Security Agency. He holds a degree with a major in English. In addition to his initial Agency assignment as a CIVOP at Herzo Base, Germany, he has worked in predecessor W organizations, at the Pacific Experimental Facility in Japan, and since 1966 in B4. He is now on a History Fellowship with the National Cryptologic School Press, and has recently been appointed to the Editorial Board of the Cryptologic Spectrum.

~~TOP SECRET UMBRA~~

비밀
한
것
이
다



IT'S CLASSIFIED !!!!

~~TOP SECRET UMBRA~~