Doc ID: 6708422

~~TOP SECRET~~ *Mr. Callimahos*

National Security Agency

Fort George G. Meade, Maryland

JUNE 1973

DRAGON SEEDS

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

This is *Dragon Seeds*.

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

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

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

Dragon Seeds is yours. May it grow with you.

The Editors

PL 86-36/50 USC 3605

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 I. Reed

Special Interest Editor

Ray F. Lynch

Composition
Composition

Helen Ferrone
Lorna Selby

PRESS CORPS

B11	Carolyn Y. Brown	B43	Mary Ann Laslo
B12	Philip J. Gallagher	B44	Jack L. Thomas
B2	Dee Ensey	B45	John E. Uzarek
B31	Jack Spencer	B5	Nancy Fournier
B32	Jean Gilligan	B61	_____
B33	Louis Ambrosia	B62	Edmond J. Guest
B34	Thomas L. Wood	B63	George S. Patterson
B41	James W. Schmidt	B63	William Eley
B42	Peggy Barnhill		

Doc ID: 6708422

~~TOP SECRET UMBRA~~

DRAGON SEEDS

Vol. 2
Nr. II

June 1973

TABLE OF CONTENTS

RYE, AN EXTENDED CAPACITY REMOTE ACCESS SYSTEM
                    by Bernie Peters and Carolyn Palmer, P1

        "Nameless indeed is the source of creation
        But things have a mother and she has a name."

                            ---Lao Tzu

        The RYE system was designed to handle a class of
problems which was not satisfactorily dealt with by
HARVEST or any other computer system current at NSA.
These problems are characterized by small size, the need
for immediate reaction, the need for intermediate human
decision before final results can be produced, or the need
for file-inquiry or information retrieval on a timely basis.

        Some examples of these problems are:

        1. Small jobs requiring only seconds on any
computer, such as evaluating a message write-out on a
single width. Any computer can compute the average
IC and the IC for each column for any one reasonable
width in seconds. If a fast, easily available proce-
dure is at hand, the analyst will use it. If no
quick method is available, the analyst may just write
a few lines on a width and "try by eye," or may not
attempt to prove or disprove the existence of width
phenomena at all. The machine method is, in general,
more thorough, more accurate and more economical, and leads
to a higher percentage of solved systems.

        2. Jobs with very critical response times. These
are high priority jobs working in close support of a read-
ing problem or a T/A development of CRITICOM significance.

        3. Series of programs which are dependent on
intermediate results for continued sequencing. The analyst
considers these intermediate results before choosing the
next program to be run, or before fixing on the parameters
for the program.

        4. Inquiry or information retrieval tasks
(usually very input/output limited). Such tasks need the
resources of a large computer with mass storage but cannot

in themselves justify such a computer. RYE permits the efficient performance of relatively large information retrieval tasks while other processing is also being done and thus avoids "wasting" the time of a large computer.

All of these problems can be handled more economically by a centrally located large-scale processor to which a large number of stations have access than by scattering a large number of small-scale computers in various locations in the building. Since RYE is a real-time multi-channel device, the stations may all submit requests and receive back results without interfering with each other.

Outstations deliver requests and data to the computer via telephone lines (NSA grey phone system) and receive results back in the same manner. Depending on the amount of equipment involved, there are several classes of outstations. A general station consists of a model 35 Teletype only; a Class II station also has a BOSTIC, or high speed paper tape reader and punch device; Class I stations have Teletype and BOSTIC and, in addition, a lineprinter (UNIVAC 1004) and other high-speed equipment as needed.

PROGRAMMING

The UNIVAC 494 is designed to be run on a real-time basis, accepting requests as the users choose to submit them and from all stations without interference with each other. It can manage itself with a minimum of operator intervention. This is accomplished by means of an extensive interrupt system and a sophisticated executive program.

Each object or worker program must be written with the following characteristics:

1. It is assembled so that it is completely relocatable in core and with regard to any facilities such as tape drives, drum storage areas, etc.

2. It uses the smallest possible amount of core area consistent with efficiency.

3. All input/output is accomplished by means of return jumps to the executive (REX).

4. No use is made of the console typewriter to request operator action, other than to complain about malfunctions.

2

5. Large programs are segmented as much as possible consistent with efficiency.

6. Properly programmed error-checks are made to prevent program failure.

7. Programs are allowed to run only for a specified number of minutes (30 during the normal work-day, somewhat longer at night and on weekends and holidays). Hence an endless loop cannot tie up a large part of the machine for a long time. Also, long jobs have to be segmented if they are to be run on RYE at all.

With these rules and some additional conventions it is possible to provide prompt service to all the outstations.

PROGRAMMING PHILOSOPHY

The programming philosophy assumes continuous use. RYE operates 24 hours a day and 365 days a year, insofar as this goal can be attained. REX is able to interrupt any program at any time between the execution of successive instructions in order to service high priority interrupts, and the interrupted program is completely unaware of the happening. Outstations may submit requests at any time the Teletype is not already tied up with another job; in fact, all terminals may submit requests simultaneously. As soon as feasible after receiving an "end-of-transmission" signal from a terminal, the system will return a receipt giving the date and time of receipt, the internal job number assigned to the request, the first two lines of the request containing the priority (if any), program name, station numbers to which results are to be forwarded, and the requestor's name, section, and telephone extension.

Programs are run as soon as possible, according to the priority of the jobs awaiting scheduling. Priority is determined by the user, with the proviso that the user will not request a priority higher than the maximum official priority of the job. The user uses a lower priority if he does not want this run to interfere with his own more urgent tasks, if he wants the output held for delivery next morning or printed on the downstairs printer, or if this is the type of research job which should not interfere with any operational procedures but which he would like to have run in any slack time which may develop before next Monday. Only in exceptional cases, and with documentary

justification by the appropriate authority, is it permissible to run a job with a priority higher than its officially assigned maximum. This officially assigned maximum is based primarily on the amount of machine time, core space and additional facilities required by the program, but with some consideration of the over-all importance of this particular task in the work of NSA.

Once a job has been placed in the scheduling queue, the program is placed in any available space in core as soon as it can be accommodated if the additional facilities required are available and if it is the first program in the queue which can be accommodated. Hence a small program may well be scheduled ahead of a larger job which has higher priority. Only in the case of a major emergency and on the direct authorization of the Chief A Group, Chief B Group, Chief C Group, Chief P1 or Chief P, are such drastic procedures as ditching jobs already in process resorted to in order to get a run started immediately. Hence, it is incumbent on programmers writing for projects with critical response times to use facilities as sparingly as possible, consistent with efficiency.

The executive runs as many programs "concurrently" as possible. This means that REX attempts to schedule as many of the jobs awaiting attention at one time as possible. Once a pro-gram has been assigned facilities and loaded into core, it can receive a share of the available running time. The oldest program in core is the first one to be considered for control. If it is awaiting the execution of an I/O request and has nothing to do, the next oldest program will be considered, etc. Thus, a small program, which "sneaks" into core in space too small for waiting higher priority jobs, may actually be completed before other jobs waiting in the queue with it are even started--and in what would otherwise be wasted time.

RYE periodically inventories the queue of jobs not yet completed to be sure that none is being unduly delayed, and takes corrective action to insure that all jobs are started within a reasonable time after their request, considering their priorities. RYE also keeps a complete log of all transactions and is able to answer queries from originators as to the status of their requests. For these purposes a unique job number is assigned to each request in strict order of receipt.

~~TOP SECRET UMBRA~~

OUTSTATIONS

The basic outstation is a model 35 ASR Teletype. This permits communication into or out from the computer at a 10 character per second rate via keyboard, paper tape reader, punch and printer. This means that very long data tapes will take an appreciable time to input, and if a station has many such tapes, it will want to obtain or make arrangements to use a BOSTIC high speed reader (300 CPS). However, it should be noted that there are no long waits for other stations to complete their turns before input can be started so that the 5 minutes it would take to input 3000 characters (or 25 feet of punched paper tape) may be preferable to walking to a station with more rapid input equipment. Also, it is possible to input a stream once and have it held for a number of runs without taking the time to re-input it--or to input a long stream and have it broken into sections with an identifier attached to each so that any subset of the whole can be selected for processing.

On the output side of the situation, whenever a large volume of output is required, it is desirable to have it printed on a line printer to avoid tying up the Teletype. This is particularly appropriate when small parts of the output are worthless or nearly worthless until all of it is available to the analyst. Four choices of disposition of results are available to RYE users. One may require that (1) output be forwarded to the requesting station only (regardless of the delay encountered before that station is on the air and free to receive--a valuable insurance for some compartmented problems); (2) one may request output to the station, if it is up, otherwise printer output; (3) output to the station, if it is not busy, otherwise printer; (4) printer output regardless, so that the station does not have to stay on the air after normal working hours or will not be tied up if a pressing problem comes along.

BOSTIC readers are able to accept paper tape at 300 characters per second and in either manual or automatic mode. They require an associated Teletype to initiate the request and receive back the receipt for the job. They can also be used for punching out long paper tape results (for example, weight tapes and crib banks which one wishes to keep on file for later input).

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

     The remote printers operate at 300 lines per minute. They normally have paper of the same size as the Teletypes (8 1/2 x 11) and can be used to provide faster output in the same format as the Teletypes. A computer printer is always available as an output device.

PROGRAMS AVAILABLE

     In addition to many specially written programs for specific projects, several General Utility Programs (Guppies) which should be of use to analysts from various areas are available. These can be divided into several groups:

    A.   DIAGNOSTIC PROGRAMS

        BIG STET--a large flexible stethoscope package which will accept up to about 100 messages and a total of 24,000 characters and which will allow the user to select the subprograms and options he wishes.

        DIANA--allowing printout of digraphic identities and statistics on ten sets of digraphs where the wanted set is specified by I, J, and K parameters. I indicates the position of the first character of the first digraph of a set, J the increment to reach the second character of the same digraph, and K the increment to be added to I and J to locate the next digraph of the set.

        INDEX--a flexible index for up to about 30,000 characters where the records to be sorted can be up to line length and cut from the stream in assorted ways; the control or sort key can consist of any 15 characters available in the record; the input alphabet can be specified by the user in any order he wishes as well as any coding which can be punched in 6 levels of paper tape; the output print format is also under his control.

        EPIC (Epictetus)--program which saves more information about the location of roughness found in columns of a write-out of message beginnings and/or endings, or in groups formed by summing or differencing groups and columns from this write-out.

        FINKSBURG will provide various level counts, etc., for 5-level paper tapes.

~~TOP SECRET UMBRA~~

B. MATCHING PROGRAMS

XIBAR permits a non-homogeneous batch of distributions to be broken down into sets so that the cross hitting between members of the set is as good or better than the average internal hitting of the whole batch of distributions.

CASANOVA

C. EDITING PROGRAMS

These programs perform a variety of editing functions on a single stream or a pair of streams and output results on command to the station or for input to another program. Functions which are provided include MASK (eliminates bits from a stream according to the unpunched positions of a mask tape), DOBE (1 for 1, 2 for 1, or 1 for 2 substitution), DROP-KEEP (drops or keeps specified codings), INDEED (inserts into or deletes from a stream according to a pattern), NEPTUNE (local transposition of elements within a given span of a stream), DELT (combines two streams by sum or difference of characters), LACER (interlaces a specified number of characters from one stream with a specified number from the other stream).

D. EXPLOITATION PROGRAMS

To make possible the exploitation of situations not readily handled by hand but easily managed by a computer.

GEEWHIZZER--locates stretches of cipher which combine with other stretches to produce plain-text digraphs to break into simple transposition cipher.

HUSK-

SCOOT-

GUPPY MOTHER SWIMS WITH TIDE
by Peggy Barnhill, B42

Carolyn Palmer *gets excited when she talks about RYE/TIDE and AUTOLINE, and well she might. She realizes how far the techniques and equipment have advanced in the past twenty-odd years, and her achievement in the field of computer cryptanalysis dates practically from the initial combination of the two terms. When Miss Palmer arrived at AFSA in 1951 with a freshly awarded M.A. in Math, the "computers" were limited to analog machines and EAM or RAM equipment.*

One of Miss Palmer's initial assignments was with a group of cryptanalytic gurus who combined their talents to achieve a seldom heard-of success--they read a one-time pad system. With that achievement to inspire her, it is easy to understand how Carolyn became one of our most dedicated succeeders.

As part of what later became P1, she also spent some time evaluating the KW-26, a piece of U.S. cryptographic gear. While that equipment proved to be a little better than that of the competition, the correction of several flaws which were found made it much more reliable...so reliable, in fact, that it still constitutes a major portion of the U.S. cryptographics inventory.

Carolyn was introduced to programming when necessity called for training a nucleus of BOGART programmers. The ensuing course, which Miss Palmer describes as comparing favorably with survival training, produced some of the best programmers we have. Its graduates put together the BOGART version of STET, a grandfather of the present-day crypt diagnostic programs.

The BOGART STET was a great advance, but a problem developed because of the program's popularity. People were using STET to make 53 measurements of a cipher stream when they really wanted only three. To solve the problem, Carolyn began the development of the GUPPIES. These short, general-purpose cryptodiagnostics were installed on ROBROY and, with little variation as capability of the system advanced, they are much the same today. While she didn't write all of the GUPPY programs, Carolyn was generally responsible for them. She is therefore most widely known as the "GUPPY Mother."

Doc ID: 6708422

        With the upgrade of the system that the installation of
RYE brought, Carolyn began to see the concepts originally
envisioned for ROBROY come into being. Not content with that
success, she began planning for what has become the TIDE/
AUTOLINE system today. Today she is planning the system of
tomorrow. And considering the advance made so far, and being
aware of her insight and what a co-worker describes as her
"unreasonably good programming ability," we are sure that
tomorrow's system will be as much of an advance over the TIDE
of today as TIDE is over the ROBROY of yesterday.

        We don't want to give the impression that Miss Palmer lives
each day to "do or die for DIRNSA;" she has other interests.
She possesses the love of good music which seems to be present
in nearly all "computer-type" people and is a regular subscriber
to the National Symphony. When her schedule permits, Carolyn
spends time relaxing in the nearby Virginia mountains or
visiting with a family whose members are scattered along the
East Coast from New York to the Florida Keys.

9

ONE CHANCE IN THREE---BUT IT WORKED
                              by William Gerhard, B6

     ARDF needs no trumpeters in B Group, in ASA, or in AFSS.
But important as the ARDF program was to become, experts in 1961
and early 1962 doubted that the first experiment involving direc-
tion finding and an L-20 aircraft would prove successful. As it
turned out, there was one chance in three that the experiment which
led to the ARDF program in Vietnam would, in fact, work at all.
The following excerpts from an interview of Mr. H. S. Hovey,
D/Ch of Staff for R&D, Hq, USASA, by Mr. L. L. Sternbeck and
Mr. J. Gilbert of ASA shed some light on the first ARDF birds
to fly for the U.S. in Vietnam; on the early improvising by ASA
innovators; and, despite odds against them, on their success.

Why ARDF was Required in the First Place

     Q. *Prior to ASA's becoming involved in ARDF development,
was there any ongoing development of the capability within the
Army?*

     A. The answer is really no. There had been, of course, a
lot of development of ADF (airborne direction finding) systems
for navigation purposes, which don't operate in the HF range and
also the FM homers and other VHF navigation systems.

     Q. *...The question I always had...Why was it so difficult
for us to do that?*

     A.   ...There is actually a technical explanation for why
this difficulty occurs...the Vietnamese and the VC were using low
power radios. Now, how do I get in HF a low powered radio...
say, a one-watt power...to transmit a hundred miles? Well, the
way to do that is to use a horizontal antenna, radiate the energy
up to the ionosphere; then the ionosphere causes it to reflect
down on the point you want. That means almost no energy is going
out directly, so you sit over here on the ground with your direc-
tion finder even a half mile away, and there is no ground wave
energy to hear. Now, an interceptor can listen because the sky
wave is coming down from the ionosphere. I can sit there and copy
what he is saying, but when I try to take a bearing, I am trying.
to take a bearing almost straight up, and there is just no way
you are going to do that. Intercept is fine from steeply incident

10

skywaves, but DF needs a much more stable propagation path. The salvation is ARDF...you get a line of sight to him essentially, and there is now enough direct wave energy for you to operate with. You still must discriminate against the vertically incident energy. That was what had defied everybody because at these frequencies the aircraft dimensions are about the same as an antenna. So then all this steeply incident energy comes down on the airplane, and the skin of the aircraft is excited with RF currents. Your antenna is coupled into it and all you get is a hodgepodge...the one great thing we learned technically was how you could make a system that decouples from the plane, discriminates against the sky wave energy, and operates on the direct wave energy. Now on the broadcast band you don't have that problem. You are talking large power and a lot of energy that is vertically polarized [and] radiated out. The same with VHF. The VHF will not come back down from the ionosphere. That is exactly why the Viet Cong used this [HF] frequency, because it did support propagation...

It was October/November of 1961 when the urgent requirement came out of Vietnam because they [3rd RRU members] had gone in-country and were trying to use AN/PRD-1s, and they couldn't. The AN/PRD-1 is a ground loop type DF set and needs a good ground wave signal to work against. A cable came back asking us what we suggested or what we could do.

The Experiment

Q. Was this the 3rd RRU?

A. Our 3rd RRU and specifically...WO George Miller. I was the project officer for direction finding systems in these days. George Miller and I---I had the action here through command channels and he had the action there---had this exchange of messages; there were probably 10 or 12 messages in that sequence. We worried about how to improve the AN/TRD-4s, which is the larger DF set and what we were going to do with his AN/PRD-1s. Then we got on to what we could do to solve it. That was where the idea of trying the aircraft emerged. We thought an aircraft would be useful, and he agreed that probably the aircraft would be great. In November, about Thanksgiving, I went over to Vietnam along with an engineer named Harold Jaffe from ECOM [U.S. Army Electronics Command].....So we went over and spent a month in Vietnam and wandered around with George Miller and the rest of the people involved. We went around on PRD-1 operations ourselves, took receivers and listened, making measurements of what the propagation conditions were.

Q. When and under what circumstances did ASA first become involved with research [and] development of ARDF? Was it a result of the 3rd RRU's recommendation? MACV's? Department of the Army's?

A. You can summarize it by saying that the way we got involved was reacting to the problem--that they couldn't use AN/PRD-1s to do the job and the proposition was "could we use airplanes?" And the answer was "Yes, we think we can."

Q. You got together with ECOM on this and went out with Mr. Jaffe?

A. Exactly.

Q. When did you bring Department of the Army into this?

A. We didn't really...this whole thing was done on a shoe-string. There were no external contracts made during this time frame; all was done in-house at ECOM. There were very few approvals obtained because we weren't talking dollar levels that required any approvals. Secondly, there wasn't a great deal of attention that was attracted in this time frame in the eyes of the Department of the Army. The 3rd RRU was calling for a solution, but it was to ASA. So it was later on that major involvement on the part of DA took place...

Q. Were the pilots organic to the unit [3rd RRU]?

A. Yes. I don't know how they came to be, but LTC Cochrane [CO, 3rd RRU, Saigon] had acquired two pilots, one a CPT Bill Simpson, who later came and worked here, and CPT Don Schessler. They were both Transportation Corps officers and didn't know anything about ASA until they came in. I believe a lot of credit belongs to them for having operated the thing.

Q. Did they come explicitly for this project?

A. Yes, that was something the 3rd RRU had arranged. We went out the first time feeling we could produce the gadget, and LTC Cochrane handled the arrangements for getting aircraft which he borrowed from a Signal Unit, I believe, and the two pilots. Later we came back with the equipment and put it on.

Q. The first planes flew in March of 1962?

A.   Right.

Q.   *How much testing were you doing there?*

A.   We were running a pretty extensive program.   In the
first place, it was a fairly simple system, although it performed
an elegant solution.   We had done work earlier with VHF ground
direction finder, a thing called AN/TRD-16, which ECOM developed,
which is composed of a pair of antennas differentially connected.
That was a very effective ground direction finder in the VHF.
That was the technology which we applied to the HF but increased
the spacing between antennas.   In terms of hardware you weren't
talking a great deal--a receiver, some cables, the antennas on
the aircraft, and a little bit of circuitry to connect them.
That was the size of it in the first version.   It was a kind of
thing which did not require weeks and weeks of fabrication.   It
did require an awful lot of testing.   A whole series of antennas
were tried to get out of the coupling problem with the airframe--
that was going on at Fort Monmouth--the actual testing.   When
we felt we had something, we were able just to use the shops at
Monmouth to fabricate antennas, cables, and other things and rush
over and install them ourselves....

Q.   *Was there any training involved by the pilots and opera-
tors?*

A.   There was a lot of training by the pilot.   This was very
demanding of the pilot because he had no navigation system which
would tell him where the airplane was at the time he was taking
the bearing.   He had to learn to fly over a point on the ground
that he could then identify on his map as he took a bearing.
The operator who was flying with him with a map had the duty
of operating the receiver.   The operator's task was not too
different from the one he had operating the PRD-1 or an intercept
position.   He had to find the signal frequency and copy it,
making sure he was on the right one.   So that was pretty much
what he was used to on the ground except he now was in a plane
and had all the risks of getting air sick, etc.   But really the
pilot was the one who had to do this by pointing the aircraft at
the target and slueing the tail back and forth, reading on his
gyrocompass while he was still over ground he could recognize.
A skilled pilot can do that very well, but this is something the
average Army aviator isn't trained to do.

When we installed the thing, we worked a couple of days
with the pilots there, refining it. We flew a lot of hours
ourselves. They caught on very quickly. To prove what we had
done, we had a hidden transmitter hunt. The 3rd RRU hid some
transmitters around Saigon and they went out and found them.

If the pilot was careful in finding a bearing, even this
first system could be incredibly accurate. For instance, during
this hidden transmitter test the system showed which side of a
road at a junction the transmitters were. We were talking even
then about accuracies of hundreds of meters.

*Q. Why were the L-20 aircraft selected for ARDF? Where in
the United States, and when, did the initial ARDF testing take
place?*

A. ....We found out that this aircraft was fairly available
over there. It was adequate for our purposes because you needed
something with good visibility; it could carry two or three people
and some equipment....The L-20 just happened to be a very nice
airplane for the purpose. The big thing was, it was available
over here and could be maintained because the MACV Flight Detach-
ment was who their people worked with in the beginning--the old
MAAG [Military Assistance Advisory Group] Flight Detachment,
actually. The Detachment had L-20s.

*Q. Was it the Signal Corps from whom we had borrowed the
early planes?*

A. Yes, it was the Signal Corps we got the aircraft from.

We had the one aircraft at Monmouth from the Flight Detachment
that we had put the antennas on and it eventually worked out very
well. That became the basis of the system we took over. We went
over with equipment to do three airplanes. As I say, this went
as luggage. I went; Harold Jaffe, the ECOM project engineer,
went; a technician from ECOM by the name of Walter Day went; and
an airplane technician by the name of Danny Shargus. Danny's job
was to mount the antennas on the aircraft. Walter Day was the
electronic technician who was to help Jaffe and me get the system
together. Jaffe and I did most of the flying.

So we had this airplane which worked well at Monmouth. We
went to Vietnam, and they had arranged three airplanes to work
with. The first plane we put it on, it worked very well. This

is the one we did the hidden transmitter hunt from. As soon as
that day was over, they took it away from us. We wanted to test
a little more, but they figured it worked well enough so that
it went into operation. We did fly some operational missions
with them for a while to make sure things were working. We
worked on the other two L-20s, but neither one of those aircraft
worked. We installed the systems and sweated blood for several
weeks and finally just had to plain give up. We couldn't make
the systems work on these two planes. The reason for it had to
do with the way the aircraft themselves are constructed. We
apparently had some type of unsymmetrical airframe current distri-
bution. As long as that is symmetrical and you can maintain a
decoupling from it, your system will work. But some of the
L-20s had been through extensive rehab. The inboard ends of the
wings had been painted more coats on the one than the other, and
things like this. When they had been put back together you had a
terribly unsymmetrical RF current distribution, and we had no way
to adjust for that at the time.

At that time, we found ourselves literally faced with the
problem of selecting airplanes. We wound up then leaving those
two which worked quite poorly and one which worked very well.
Aircraft tail #5682 was the good one and #33731 and 37963 were
the poor ones. We came home and chose airplanes. ECOM sent
people--Walt Day, I believe, from airfield to airfield finding
planes which had not been through this major rehab, equipped two,
tested them here, loaded them on board an aircraft, and flew them
out to Vietnam to give the 3rd RRU the three it was after. The
planes they had which didn't work well went back to where they
came from. The 3rd RRU wound up then with three working L-20s
after that ordeal. Actually, the ECOM lab A/C #55151 and #82012
were the ones that were sent out.

Now, I said there was divine intervention. It turned out
historically that one out of the three aircraft worked success-
fully with this system on it. So the odds were very much in favor
that we would have gotten a bad plane in the beginning at Monmouth
or that we should have gotten a bad plane in the beginning in Viet-
nam. Given the suspicion (or skepticism) about ARDF--we could
have very well stopped, had that happened--and here very competent
people had said it couldn't be done anyway. There may not have
been such a thing as ARDF today. It was a fortuitous thing and
something we speculated about.

Doc ID: 6708422

Q. *Do you have any...anecdotes related to the development of ARDF...?*

A. I think this business of taking it out as luggage. And the pilots would have been far more worried than they were if they had known just who mounted some of these systems, because all of us wound up riveting things on airplanes. I did. We almost lost it all in Hawaii when they misrouted all our luggage. We had to go at the last minute and dig that out of another Pan American aircraft. I think the selection of aircraft is also significant.

One of the things we took some technical satisfaction in was a little event out there when we were flying the first one. What we would do was to fly to Bien Hoa where we had a DF site and the flash transmitter which controlled our DF nets in Saigon. So we would fly over our DF site at Bien Hoa and shoot that flash transmitter, taking a bearing on it because that was one of the check bearings they used that was supposedly quite accurate. We worked a couple of days because there were a couple of degrees error, and finally in disgust went back and recomputed the check bearing and found out it had been calculated wrong and that the aircraft had been correct all this time.

****

"The Wise Man, when abroad,
Impartial to the world,
Does not divide or judge.
But people everywhere
Mark well his ears and eyes;
For wise men hear and see
As little children do."

---Lao Tzu

16
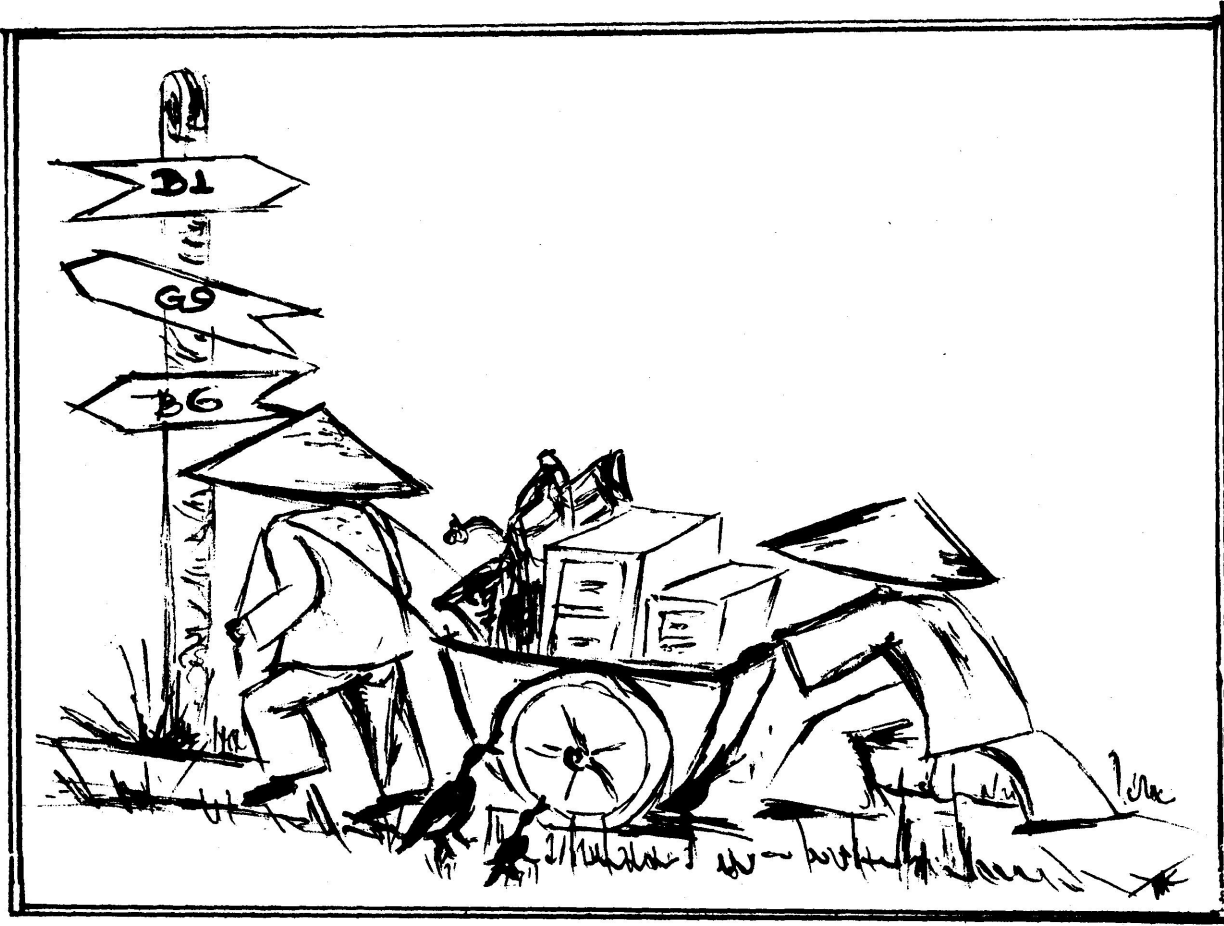
"The gem cannot be polished without friction,
nor man perfected without trials."

MARKETING OUR PRODUCT
                    by Walter D. Abbott, Jr., B6

     Many of us involved in the production elements of this
Agency have heard the expression, "Product is our only product."
The capabilities, successes, and even the shortcomings of our
intelligence apparatus are amply documented by the myriad of
products released by this Agency on a daily basis, and overall,
speak quite eloquently for the talents, dedication, and technical
skills of the people devoted to intelligence production within
NSA.

     Recognizing that we are dealing with a fluid cast of product
recipients (many of whom may only recently have become involved
in the intelligence business), and recognizing that some of our
subjects and jargon might be considered technical, confusing, or
perhaps even mystifying to the casual reader, we have set up a
system of user service centers, known variously as Cryptologic
Support Group (CSG), NSA Operations Group (NOG), and Intelligence
Support Staff (ISS), to assist the user in understanding and
interpreting the product he receives. These organizations have
often demonstrated their functional utility and have periodically
reflected quite favorably on NSA. The quality of these opera-
tions has not, however, been consistently excellent, and this
is the point I intend to address.

     The success of any product service operation is contingent
on the people manning the operation. Most of our operations
located at major command headquarters outside the Washington area
are manned primarily by NSA civilians whose function is to
advise and support their military counterparts. For many military
personnel, the people they meet at the product service organiza-
tion will be the only NSA people they will be exposed to during
their military career, and the impressions they form of the Agency
itself will be influenced by the impressions they have of the
NSA people they have met. It is therefore extremely important
to give these command personnel the most positive, favorable,
impression we can.

     We ostensibly endeavor to ensure that this happens. We
select personnel for the product service organizations who are.
generally very knowledgeable on some target entity, have a demon-
strated talent or skill, and are considered "experts" or "near
experts" in their field. This is, however, only one part of the

selection process. We also select people who need a job change for professional or career development reasons; people who are the only candidates for a particular position (at which time skill, talent, etc., become secondary); or people who have either never been overseas or have not been overseas in many years. In recent months a prevalent opinion is that this latter criterion is an overriding factor in overseas selection.

We normally do not select people because they have performed such jobs in the past and demonstrated real skill at handling such jobs. We do not have, for instance, a cadre of overseas specialists who not only are SIGINT specialists, but also are versed in command structure and relationships and capable of doing a good job in a command environment. Rather, we endeavor to "spread the wealth" and by so doing, we sometimes end up a bit poorer than when we started.

I am not condemning the system as it exists. I am merely offering suggestions which I feel might improve it and give the Agency a better image overseas.

First, I strongly advocate that at least some selections be based on past performance in the field. If a person has demonstrated an ability to represent NSA with excellence, he should be allowed to serve again as soon as possible or to continue to serve if he is already on the job. I know and know of several individuals who have done truly outstanding jobs overseas, who were functioning well, were happy where they were, and wanted to stay but had to come back to NSA because their tours were up. They had little or no prospect of returning to the overseas area. Excluding the cost considerations (the expense involved in rotating families is not insignificant), the Agency opted to replace a known commodity (i.e., a man who was a good Agency representative) with an unknown (or at least untested) commodity for reasons which to me are less than clear. I suggest the system needs to examine its inflexibility and consider each man on a case-by-case basis. The result should be beneficial to the Agency, and that seems to me to be the paramount issue.

My second recommendation is that all NSA personnel, before they are sent to an overseas job which demands continuing exposure to non-NSA personnel, be given a series of training courses dealing with personal interaction, as well as command relationships and responsibilities. Too often our people forget

that the person in the command intelligence shop is frequently new to the business and may have been a weapons system operator for ten years before being given a Special Intelligence clearance. Questions from that individual might seem stupid, trivial or a waste of time to the NSA person who has been involved in the cryptologic business most of his adult life, but he should attempt to answer them without condescension. Moreover, the NSA people should get to know their counterparts and be able to relate to them, on and off the job. Superior, aloof, indifferent, and arrogant attitudes have no place in our overseas operations. But they exist and they hurt us. We should expend all necessary efforts to develop a sense of trust and confidence in the people we support. If that can be achieved, the entire support operation of the Agency will benefit.

The training program should include a little "Madison Avenue" public relations training and a brief exposure to salesmanship. It is not enough to be a good analyst, technician or reporter. The individual also must be a good representative of this Agency, able to convince his command counterparts that our product is worth their attention, and that we honestly want to satisfy the command requirements, regardless of our individual propensities. We have a very saleable product. We need to develop the personnel to promote our product. It might be worth the investment for the Agency to explore various industrial programs geared to developing a sales force. The "foot-in-the-door" syndrome has applicability in our business, and developing a training program to foster this is, in my opinion, both worthwhile and necessary.

Again let me state that I am not faulting the existing system so much as offering ways in which it might be improved. We have a good product and a ready market for it. Let's market it properly, and make friends for the Agency in the process. Let's do it right.

Transposition is...

This month's puzzle has pairs of twists.   Can you solve it?

```
G E R T M     C U S E L     A E P I M     S F T O N     S E I E A
U N D N I     H U D R F     Y H O R I     E H O N L     I E P A U
V E E E U     N F M F O     E W T Y W     O N T N O     O T R I X
A E L E E     N M G E F     U K O I I     H T E T E     D H N G I
I T A W M     K E A R E     E H N R S     E V S A R     E T R A F
T S I N A     E L L Y N     H A E D X     M O R I D     Y R U X N
O E T I I     N N S X S     L G F N T     O E I S S     H D D W N
S A L F T     P X I U I     V I U E R     O A M E D     H N E N A
X R R A T     E I I W C     D N T R D     A U O I K     D S A E R
O R H E H     A O T T P     G N E E G     L T R M E     S N N F O
S I T S H     E T A O A     S P L Y O     E U S H M     D E X N S
S C E L N     R A A A E     D P L Y I     U O E O N     E A T E C
H I O E T     R N S O X     I T B A T     O L R D M     O H O S A
D O C S X     S O O S E     I O N S L     U O S T D     H L D T A
E X A S V     E N S B S     U P A D I     E D Y E N     T C E A E
T T M H V     H R R X R     C D T E R     T H C N X     E F P L A
D H G O H     G T T O D     T E B C O     R M T U O     D M R M P
A T U A D     N I D W I     F R I R T     I C I O H     S E E E I
A X T E T     H W O R E     A T I V L     L E L I E     S F E A I
Y H C S F     I L I F X     E P T R N     M S O X R     D P L E A
S E D R T     H Y E O T     S L W I M     R M C B N     O I G S P
T W L O O     I E I R F     T N F A D     O O R S N     M E H T S
O T L F I     S P N W A     C G B E I     L T C T I     E S A B H
O M M A D     U F O N L     E H A H M     S T F N I     I H O E I
G N M O O     O I F G O     E P O A G     W B D C C     L A A X S
S Y T N H     G S N A S     O O T D N     S L X N A     D D A S E
I S N H I     I S T L T     H C O O E     R S A H T     E M N O V
A A L C A     Z U K A O     T A M E T     C S N E U     L E E N R
T C T D N     U N O A R     F L H R I     G F D L C     R A N M T
O N A H T     I S H E R     O M E E S     D K S H N     I I L O W
S R E E E     Y R I T L     O O U S X     F C E D I     T E O X I
N E S E H     O E I N N     T S N T N     S Y D Y D     S E N T N
G S N E E     O D E O T     A T E N N     H
```
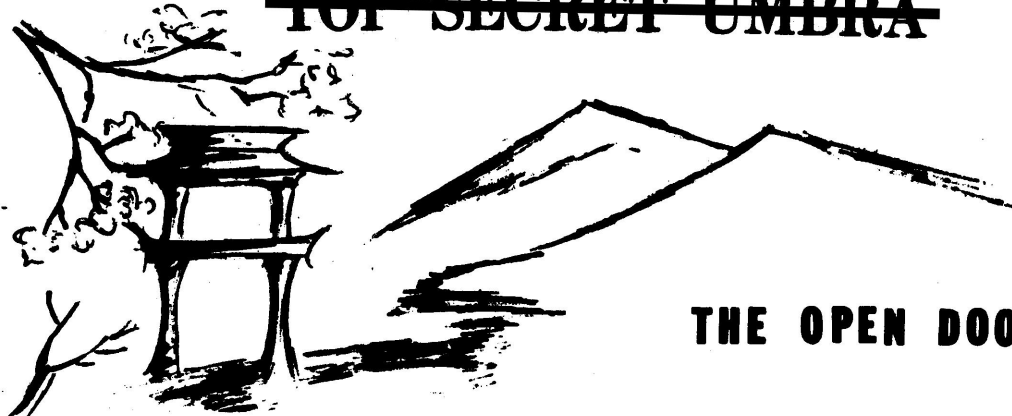
THE OPEN DOOR

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

THE "C" PARALLELOGRAM, OR A VIETNAM COVER STORY
by Bee Kennard, P222

"Lessons Learned in Vietnam" was the title of an army publi-
cation describing the latest combat developments in the ground
war. SIGINT learned many lessons there as well; but for the most
part, the participants have been too busy fighting to bother with
writing about their experiences. The Vietnam war was also an
education for the information analyst providing battlefield
support. While the lesson is still fresh and the topic timely,
this particular contribution to the war effort is believed worth
sharing and passing on.

The Monsoons Came

Times have changed since Napoleon, for a modern army travels
on paper. It simply cannot function without a piece of paper
telling it where to go and what to do and how to do it. The
Viet Cong/North Vietnamese Army had paper, paper everywhere.
Torrents of infiltration passes, invoices, manifests, supply
lists poured down the Ho Chi Minh trail. Files, records,
accounts, inventories, manuals, directives flooded the base camps.
Marching orders, firing tables, target studies, attack plans
swamped the battlefields. And floating on top of the official
paper sea were the personal diaries kept by every VC soldier from
private to general. If the info analyst could survive the
innundation, captured enemy documents made Vietnam an intelligence
paradise.

22

The Communist proclivity for secrecy compounded the red tape because everything and everybody had a cover name which changed constantly. A drifting cover designator list became a lifeline for the drowning analyst to latch onto. Studying for dear life, the cover designator lists revealed an identification system that was intricate, minute, and precise. There were two main channels, military and party, and each had a four-part cover address consisting of a cover name, a cover number, the official letter box number, and the personal letter box number. Every military unit from division to company had the four-part code which was different at each echelon. The party organization and its agencies at the district, province, and regional level were assigned a multipart cover address. There were separate sets of cover designators for intra- and inter-regional correspondence and between North and South Vietnam. The party used family relationships to denote echelon while the military used the government administrative structure. Leaders favored numbers for cover names. The VC cover system was controlled from the top and carefully regulated. Once the patterns were mastered, the info analyst could knife through the complicated tide with ease and dispatch.

Communications Problems

Buoyed with success and armed with the trustworthy VC cover system, the info analyst turns next to bail out the SIGINT analyst. However, SIGINT has its own identification system for VC targets, and in another language yet: radio station designators, case notations, crypt systems, callsigns. The two systems would not mesh. Not only do SIGINT and collateral not speak the same language, but also there is unreasonable doubt that the two are even in the same ball park. What can you do with a can of worms that $w_r i g g_1 e\ o_f{}^f\ _i n\ ^a_1 l\ d^{ir}_e c_t{}^i_o n^s$? Common sense to the rescue. The first step was to set up two columns, SIGINT and collateral, and jot down just the bare facts under either heading. This move put a stop to the confusion over nomenclature. Lined up side by side, the next step was to match the VC cover with its SIGINT counterpart. Some pairs were easy to hitch together, but others balked and got downright obstinate. So we applied psychology. Any analyst handling voluminous material over a lengthy period develops a feel for his subject, but these feelings are seldom expressed or written down. This intuitive knowledge spells the difference between success and failure. Altogether, the parallel format, the fusion technique, and the inductive approach proved a sensible, workable arrangement. A number of secret VC targets were identified.

Parallel Construction

Here is a shining example of what this device can do with a really tough problem. The story uncovered by your war correspondent has everything: action, suspense, mystery, intrigue, a devious plot with a surprise ending, and a search that ranges from steaming jungles to elegant drawing rooms and races to a thrilling climax at zero hour in a mountain hideaway. Since the facts do not always speak for themselves, interpretive comments have been included to aid the uninitiated. Lights, camera, ACTION!

Collateral	SIGINT

C mentioned briefly in directive on expansion and development of crypto branches, Region 1.

C from content apparently crypto agency on higher level than COSVN (Central Office for South Vietnam), the VC head organization.

Date of info: 3 Jan 66
Source: captured document
Comment: An unobtrusive beginning.

C both sent and received messages.

C messages more strategic than those addressed to R (cover designator for COSVN).

C cadre operated command post in (VC) Military Region 3.

C radio operators and crypto personnel infiltrated to MR3 in Aug 1970.

C radio equipment dispatched to MR3 Oct 70.

Date of info: 1969-70
Source: captured message register, code books of Signal/Crypto Branches, MR3
Comment: ARVN J2 study dtd 11 Mar 71 established that:
·C does exist.
·C is different from and higher echelon than COSVN.
·C has operated in delta region of SVN since at least 1968.

Comment: Communications links between MR3 Hq and High Command were the same as those with other known military regions. Until Oct 71, MR3 Hq continued to use a signals plan involving callsigns from a system which was

24

Collateral	SIGINT
Conclusion: ARVN J2 opined that Agency C is the Forward Command Post of NVA High Command, Hanoi.	generally replaced in late 65/ early 66. An unusual feature which could not be explained.

SIGINT continued:

Col Nguyen Van Sau to return immediately from Front 4 (in Danang area) for urgent work with General Staff in Hanoi. Car transportation arranged.

Date of info: Apr 71

Source: Intercepted message of 559 Transportation Group.

Comment: To spell out the full name in traffic is never--well, hardly ever--done. This rare occurrence constituted a real breach of security. The colonel must really be important to rate a private automobile in transport-scarce North Vietnam. Could he be the same man found in collateral?

Collateral continued:

Nguyen Van Sau signed leave authorization for command of CP.40, Central Executive Committee, Lao Dong Party.

Date of info: 17 May 65

Source: captured document

Comment: An innocuous tidbit-- but follow where it leads.

CP.40

Commander: Lt Gen Nguyen Van Vinh

Location: Hanoi, 96 Quoc Tu Giam Street

Mission: Secret military command center directing Liberation Front activities in SVN.

Organization: Diplomatic Office
Planning Office
Civilian/Military Affairs
Finance/Economy Office

Date of info: late 1966

Source: VC POW

Collateral   SIGINT

Comment: The plot thickens.
Isn't it incongruous for a military
outfit to engage in diplomacy? Or
is CP.40 strictly military? What
business does the finance office
transact?
   Central Reunification Committee
   Chief: Lt Gen Nguyen Van Vinh
(See above for connection.)
   Mission: Executive agency of
Politburo. Directs and coordinates
all military and political activ-
ities in SVN. COSVN is responsible
to CEC thru CRC. Staff Hq for
conduct of Liberation War in SVN.
No communications of its own.
Ministry of Defense provides all
communications facilities.
   Date of info: June 67
   Source: VC rallier
   Comment: If the CRC uses the
military communications system for
the military side of its mission,
then it could use party and dip
comms for its political and diplo-
matic functions. The scene shifts.

3 Jan 69, new routing desig-
nator on traffic from Special
Delegation in Paris. Msg
relayed to COSVN by CEC, Hanoi.
Feb 69, new routing designators
on Paris messages for both Hanoi
and COSVN. Then two more groups
appeared: Phnom Penh-Hanoi-
Peiching, and COSVN-Hanoi-Phnom
Penh.
   Any msg originated by one intend-
ed for other two.
   Phnom Penh link last observed
Apr 70 following break in dip
relations.
   Hanoi and Paris messages pre-
dominate. From SIGINT viewpoint,
the new designation system on
dip-party comms is unique because:

Collateral   SIGINT

1. Routing designators in addi-
tion to and different from dip
mission designators.
2. Msg technical characteristics
similar to but unlike dip post
comms.
3. Msg between foreign NVN
embassies is infrequent.
4. COSVN involvement with NVN
dip posts for first time.
Source: 2/OO/VCD/R14-72 dtd
17 Oct 72
Comment: To sum up, we have an
organization which used the dip
crypt system and the dip communica-
tions network but is not part of the
dip establishment. What organiza-
tion fits this description? The
Central Reunification Committee.
The CRC has a man in Paris and
with COSVN and had a man in Phnom
Pehn and Peiching. CEC, Hanoi,
which relays the Paris messages,
is the diplomatic office of the CRC
and the triple axes were the CRC
dip communications net. An excit-
ing development! We're off in hot
pursuit.
Footnote: For what it's worth,
the defunct PP-Hanoi-Peiching axis
is believed the Finance Office of
the CRC. It costs a lot of money
to wage war. When the mob sacked
the NVN Embassy, they really came
out of the woodwork. Cambodia was
the principal supplier for the
Liberation Army, and Chinese aid
to the VC was funneled through Cam-
bodian ports. Doan 17 was the VC
covername of a secret rear service
group located in Phnom Penh. Its
supply operations and finaglings
in the international money marts

Collateral

SIGINT

was a tightly held secret. When the Cambodian source was cut off, the VC became so desperate that maritime infiltration from NVN was again attempted. Remember those trawlers?

Map, showing observation points on Bach Ma and Ba Na mountains north-west and southwest of DaNang.
   Date of info: Dec 68
   Source: French newspaperman from Vietnamese delegation sources.
   Comment: Just a nondescript map; but why that particular area of South Vietnam? What is the French connection with Region 5? Here was the key to the mystery in the answer to those two questions.

On 6 Mar 70 four new routing designators appeared on Paris-originated correspondence and were subsequently relayed by CEC, Hanoi to Region 5 Committee and Tri-Thien-Hue Committee. These Paris messages are usually passed one or two days after the Thursday meetings. The correspondence was not re-encrypted in a party system, but remained in the VC dip system.
   Comment: A communications anomaly. Why should two subordinates of COSVN receive info copies? Or are the Paris msgs intended for a special office located in Region 5?

Cover designators for high level agencies:
   Ca (elder brother) Dai-Central Party Hq
   Cau (uncle) Ca-Central Reunification Committee
   Cau (uncle) Vu-Central Military Affairs Party Committee

27a

Collateral   SIGINT

Address of C Command Committee:
        c/o Gai Lai Provincial Unit,
        Darlac Provincial Unit, MR5
    Date of info: about Mar 67
    Source: Master list of CD-LBN
designators for MR5 and MR6 classi-
fied (VC) Top Secret. Captured
from postal battalion.
    Comment: A prize document worth its
weight in solid gold. It is the only
CD list which gives the covernames of
Lao Dong Party agencies. In our par-
lance, the document would bear the
caveat HANDLE VIA COMINT CHANNELS
ONLY because in VC practice only
communications personnel had access
to master CD lists. Agency C has a
command post in MR5 as well as MR3.
Is Agency C in both regions the
Central Reunification Committee?
    "Cau Ca" personnel roster. No. 2
man is political officer of "C."
Nine regroupees assigned to 5
provinces in MR5.
    All hard-core Communist cadre
admitted to the party between 46-50.
    Date of info: 18 Sep 67 or 68
    Source: captured document
    Comment: The clincher linking C to
Cau Ca and the answer to the French
connection with Region 5.
    Premise: There exists in South
Vietnam a deeply hidden top level
decision group directing military
operations.
    Basis: Inadvertent disclosure by
NVN delegation in Laos.
    Date of info: July 62
    Source: The definitive study
"Viet Cong," by Douglas Pike.
    Conclusion: C aka[1] Cau Ca aka
CP.40 aka Central Reunification
Committee is the hidden group which

[1]"also known as"

28

Collateral   SIGINT

has been running the war all these
years.
   Comment: EUREKA! We finally blew
their cover. The very name reunifi-
cation is its own proof. No wonder
the CRC went to such elaborate
lengths to hide its name all these
years--and successfully, too. The
revelation does not materially
change the tactical outcome of the
war, but it certainly alters the
entire strategic concept. Although
the discovery came too late to help
win the war, the knowledge may help
to secure the peace. Following the
signing of the ceasefire agreement,
Le Duc Tho remarked that "reunifi-
cation" is the postwar goal of North
Vietnam. President Nixon hopes to
persuade Hanoi to achieve the goal
through political means.
REUNIFICATION is still the name of
the game.

                                   Epilogue: The Central Reunifica-
                                tion Committee could not be isolate‹
                                in SIGINT because it had no communi
                                cations system of its own. Since
                                the military, party, and diplomatic
                                systems employed by the CRD were
                                unreadable, the CRC could conceal
                                its identity but not its existence.
                                The oddity here, the anomaly there,
                                the unique and different in communi
                                cations behavior, attested to
                                something passing strange. SIGINT
                                could tell what it was not, but
                                collateral told what it was. It
                                takes both negative and positive
                                evidence to prove the truth. Prov-
                                ing the negative is a grubby,
                                thankless task and SIGINT had the
                                harder part. Neither SIGINT nor
                                collateral alone could have identif‹
                                the Central Reunification Committee‚
                                but together they found it.

After Action Report

Now is the time for a performance appraisal of the "parallelogram," focusing on how and why it works. First, note the striking format and how it clearly delineates the problem, throwing the known facts and gaps in sharp relief. The simple act of placing the facts side by side causes the sparks to fly upward. The parallel arrangement is all important for generating analysis and research. The analyst can tell at a glance what is missing and get straight to the point. Research will be a coordinated and directed effort instead of a hit or miss operation. With the whole picture before him, the individual analyst can see where his contribution fits and can better appreciate the group endeavor. To know your work has meaning and value in the compartmented world of intelligence gives a big lift to morale. Also, the parallel format provides an incentive for the individual analyst. Who can resist adding his piece to the puzzle?

Next, notice how SIGINT and collateral meet, understand, and reinforce each other. There has been limited fusion of SIGINT and collateral, but essentially each sticks to its own narrow track. No hits, no runs, no errors and no ball game. The info analyst who sees both the collateral and SIGINT viewpoints from the Agency's vantage point can build the bridge of understanding and get the two sides together to play ball. The fusion of the two viewpoints enlarges the vision, doubles the knowledge and resources of each side, and benefits the intelligence community as well. Fusion would soon remedy the execrable writing which afflicts SIGINT reporting. Why should the reader be forced to interpret what you mean standing on his head? If you can name the target instead of referring to it as an "unidentified high level authority," your sentence automatically becomes taut, crisp, and clear. Good riddance to bad weasel English would enhance our product and relieve our long suffering customers.

Finally, study how the inductive approach resolved the dilemma and untied the knot. As long as you are adding two plus two from either column, deduction can easily arrive at four. When you are dealing with unknowns (which is the usual equation in intelligence), you have to put the cart before the horse. However, the French inductive leap proceeds from Sherlock Holmes plodding. Just suppose the answer is five and eh, voila! see how she runs. Once you try looking in a new place the leads

will turn up and things start to click. Suddenly the light
flashes on. You see the whole brilliant picture, you hear
events falling into place, and you feel how every detail fits.
It's a brand new ball game! To play in the big leagues requires
a free style in analytical research. To succeed, you have to
try harder but you will never know until you try. What have
we got to lose but our ignorance?

Wave of the Future

The "parallelogram" has been tested on the battlefield and
proved a practical and valuable tool. It is not a shortcut to
success nor a substitute for work nor a formula to replace
thinking. Indeed, analysts on both sides will have to hump to
meet the high standards. No longer can either side go it alone
or afford the luxury. The "parallelogram" is a sophisticated
tool designed for qualitative analysis and research. With such
specifications it is tailor-made for subtle, complex intelli-
gence operations demanding integrated research in uncharted
fields. Pioneering is for the brave, the bold, and the
imaginative. Soaring on gossamer wings of faith and courage
with the beacon of hope lighting the way, together we can meet
the challenges of a future bright with promise. We recommend
the parallelogram as the wave of the future. It's simple,
it's beautiful, and it comes with a money-back guarantee.

*EDITOR'S NOTE: The above article has
provoked comment among the editors and
staff--not all favorable. We present it
to you substantially as it was written in
the interest of our "Open Door" policy. But
we, and the author, would sincerely appreci-
ate your comments on the article, the
intelligence "fact" discussed, and the "new
technique" represented by the parallelogram
presentation.*

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. L A T I C E D   Measure of 2's roughness.
    _ _ _ _ O _ _

2. P H O N O G R A M   See 1.
    O O _ _ _ _ _ _

3. I C R A V E A G E   Width test on STET.
    O _ _ O _ _ _ _

4. M A G G I E S   Measure of deviation from normal.
    _ _ O _ _ _ _

5. B L E A T S   Rye program which generates tailor-
    _ O _ _ _ _   made mathematical tables to YOUR
                                       specifications.

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

Print CRYPTOANSWER here.

_ _ _ _ _ _ _

ONE WAY TO GET A RAG MAN.
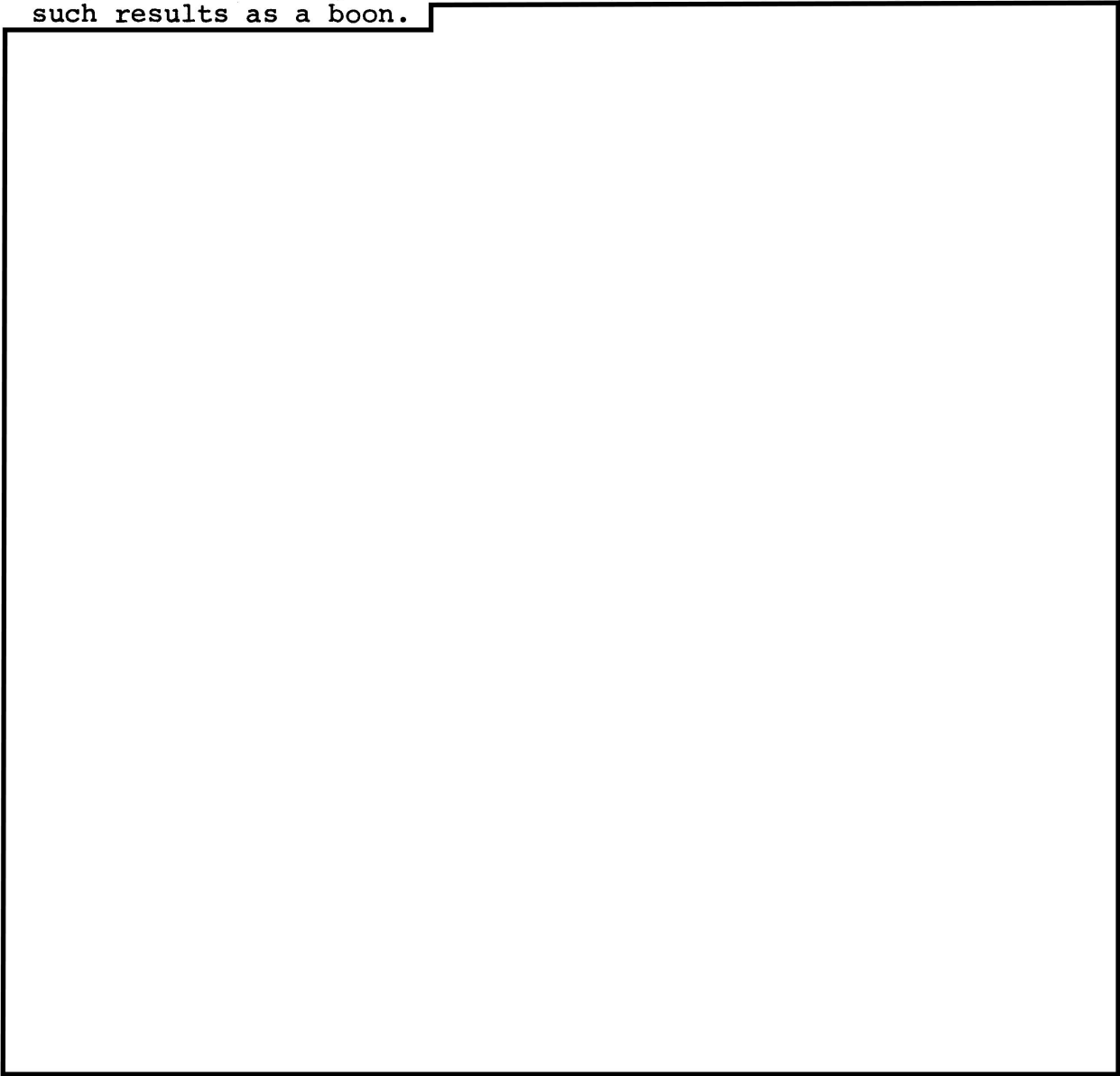
REFLECTIONS ON A NON-RANDOM BANE
by Rodney Forbes, B43

The cryptanalyst usually keeps his eyes open and his computers searching for non-random phenomena, and regards such results as a boon.

~~TOP SECRET UMBRA~~

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

~~TOP SECRET UMBRA~~

35

Wife sells
husband

BANGKOK, 27 May—Police at Nonthaburi Precinct Police Station Saturday disclosed a bizarre story to the local Press: A woman came in Saturday morning to file charges "of fraudulent practice" against another woman for non-payment of money after she sold her husband.

According to police, Mrs Somporn Sukhonghapol claimed that Mrs Somthavil Aekchart recently agreed "to buy" her husband at an agreed price of 8,000 baht (about 400 US dollars). Mrs Somporn said she agreed to take 2,000 baht (about 100 US dollars) in cash first, with the rest of the payment in the form of a post-dated cheque.

However, when she went to the bank to cash the cheque Friday it bounced "and Mrs Somthavil refused to settle the payment".—NABIAFP

EO 3.3b(3)
PL 86-36/50 USC 3605
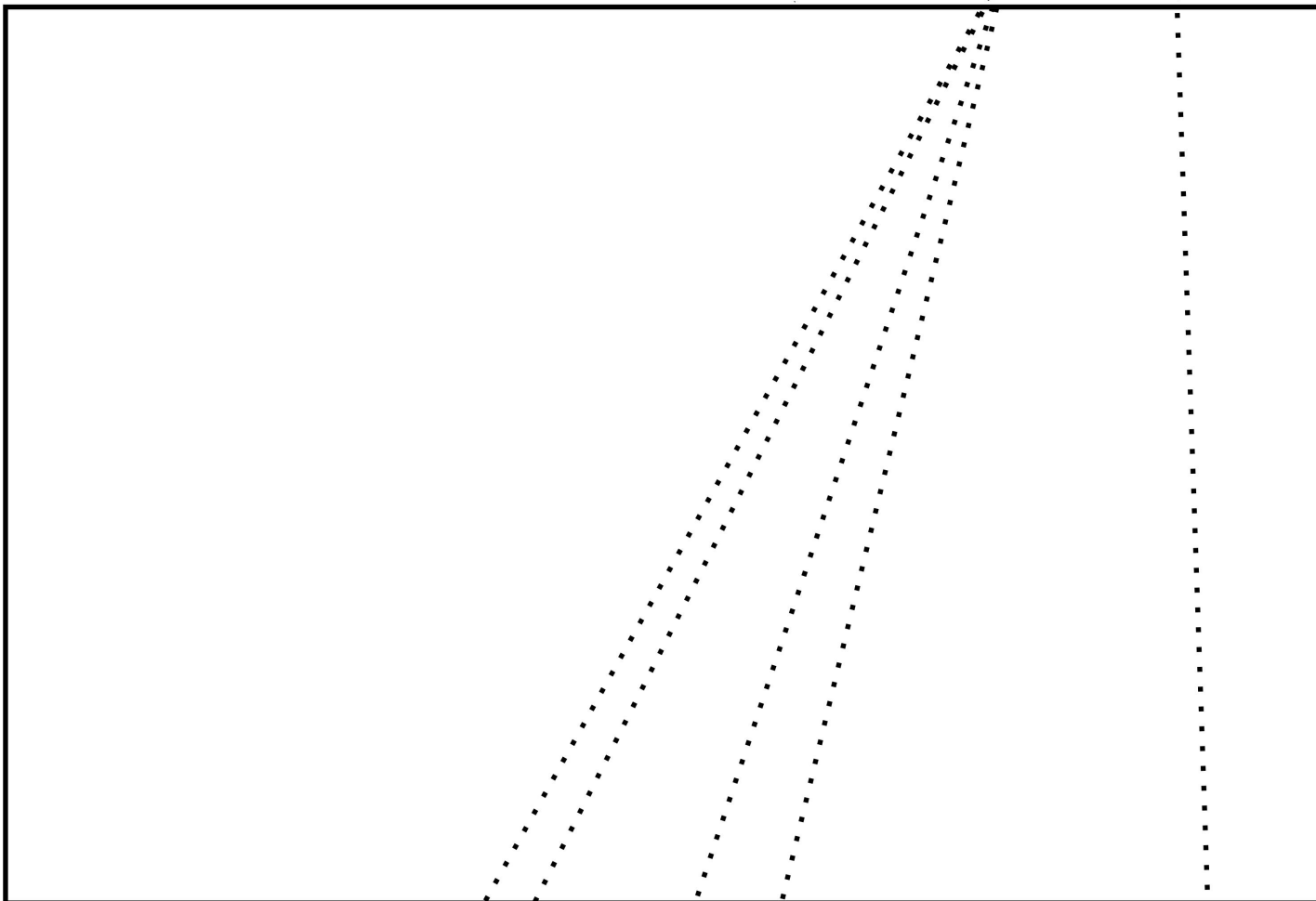
You may ask: "What is this grotesque thing above, fluttering as the page trembles in hand..."

Pulling out the ole Thesaurus, we find that it is most often referred to as an insignia, or a symbol, crest, shield, and possibly even a badge. Putting aside the fine printed pages, we find that the definitions fit rather nicely.

The [   ] as pictured above, was recently selected by a majority of votes in the [   ] (B1224) among an enormous four and a half entries to reign as the section's symbol. Whereas each entry contained technical aspects of NSA's policy aiding in the enrichment of the [   ] lives, the winning emblem, which was conceived and drawn by Sgt Frank Frate, delves into the aesthetics of the country and the people.

Referred to earlier as a grotesque picture, a correction must be made. In black and white, the symbol is misleading; however, as the emblem is posted in B1224, one can easily view the [   ] [   ] which symbolize the color and beauty of the country and especially the people.
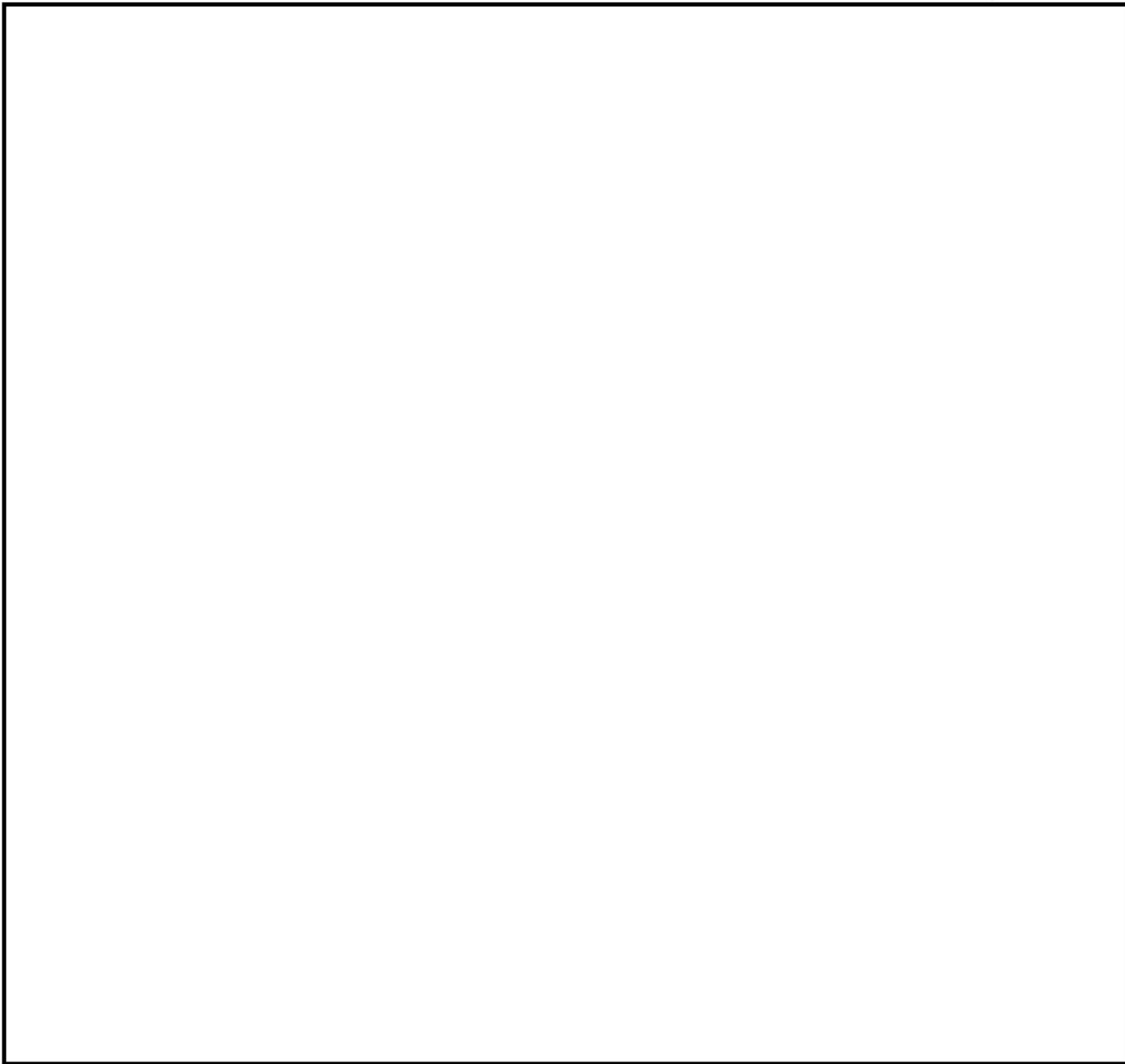
37

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

A HITCH-HIKING CIPHER
by Mary Ann Laslo, B43

~~TOP SECRET UMBRA~~

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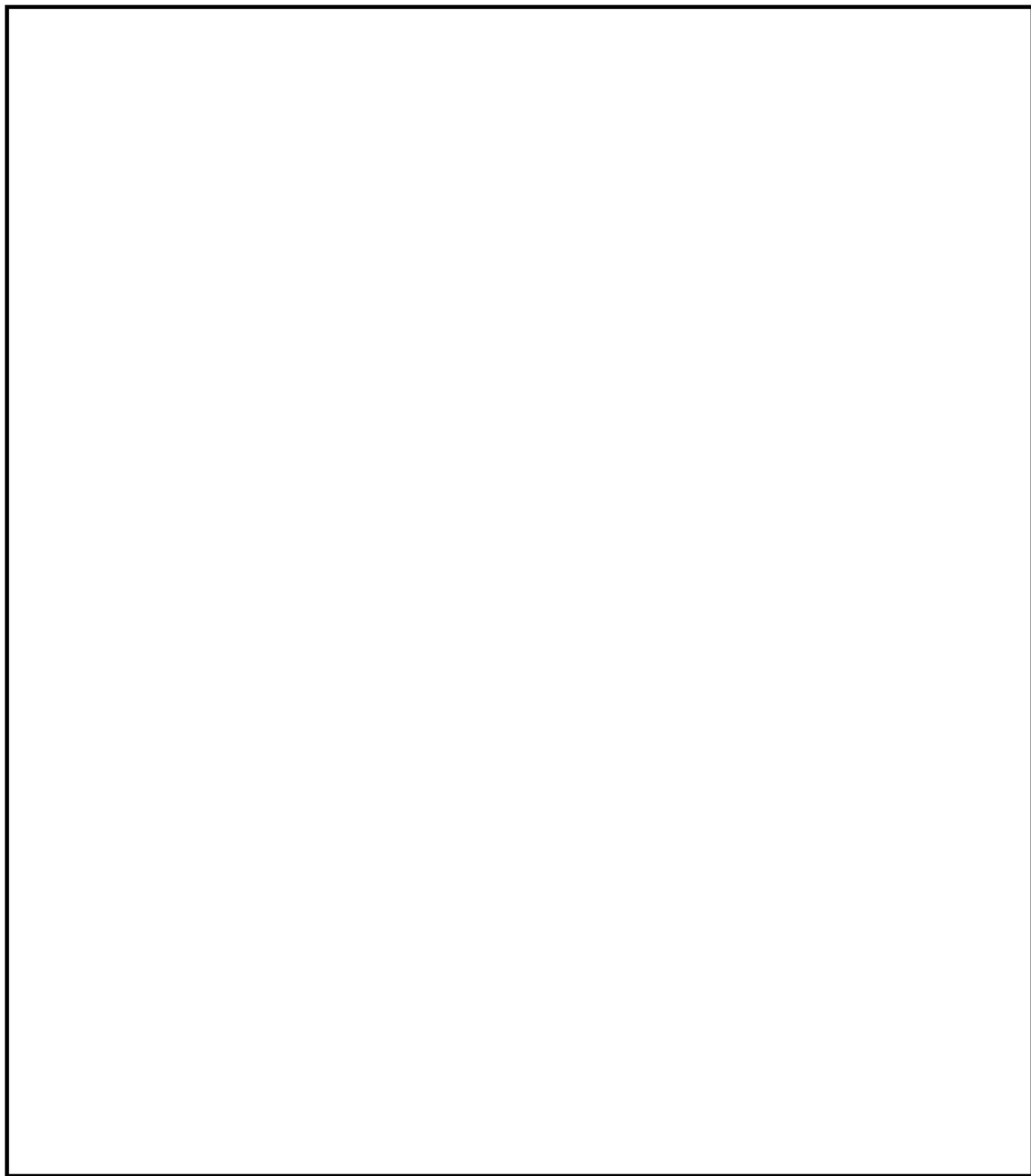PL 86-36/50 USC 3605

~~TOP SECRET UMBRA~~
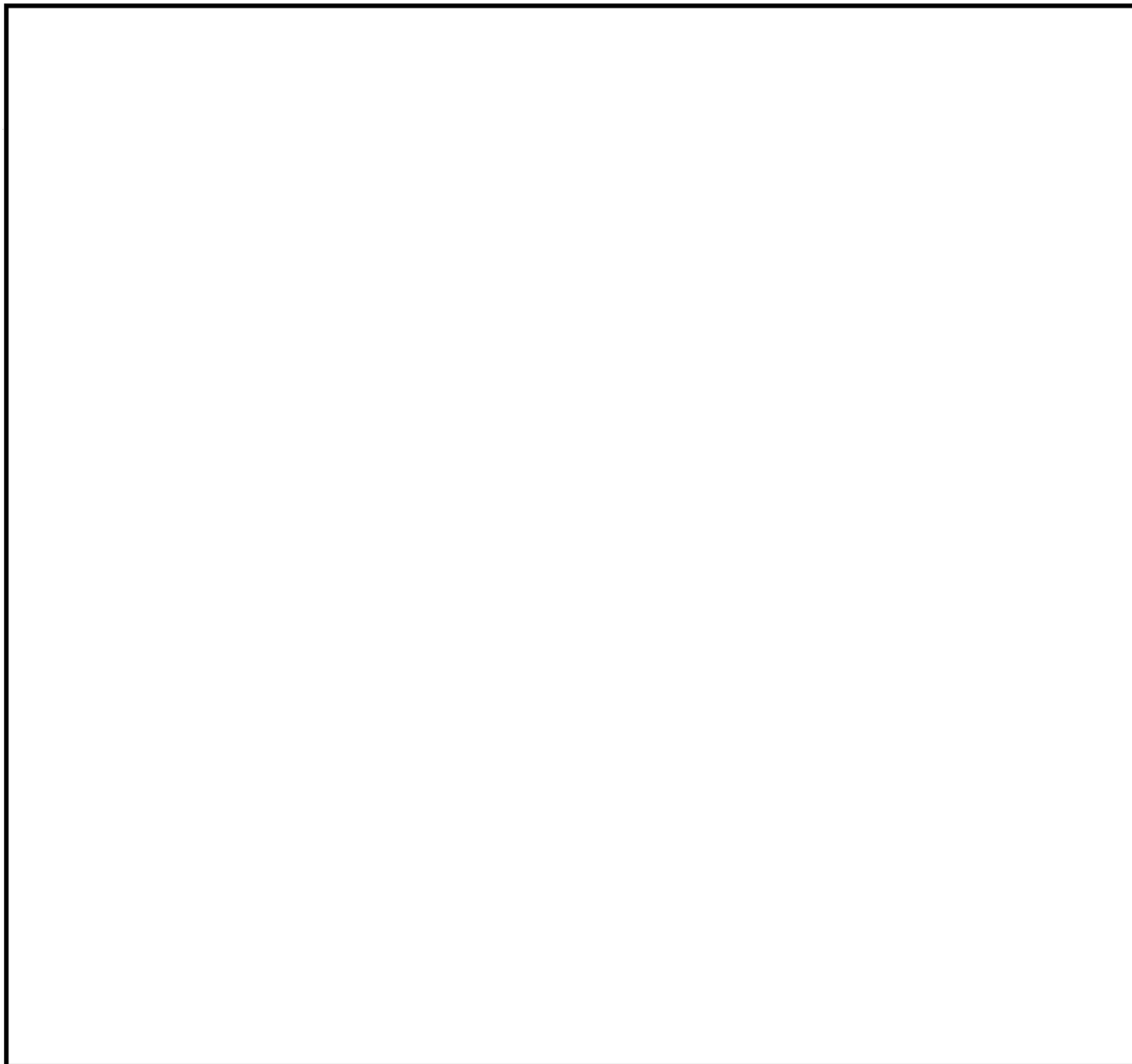
~~TOP SECRET UMBRA~~

40

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

~~TOP SECRET UMBRA~~

42

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

43

~~TOP SECRET UMBRA~~

* * * *
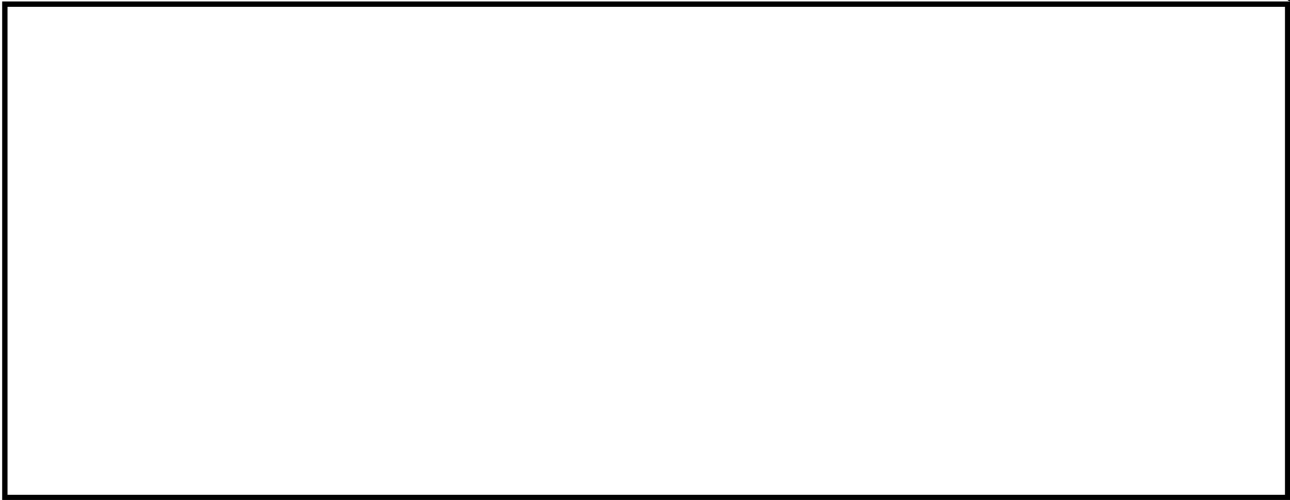
A thousand thanks for your articles!

~~TOP SECRET UMBRA~~

PROBING A NEW TECHNIQUE: CRIB DRAGGING IN SINGLE TRANSPOSITION USING DIGRAPHIC WEIGHTS

by Dr. Marti Branstad, P1

This is a report on an experimental examination of crib dragging as a technique for breaking into single transposition. Cribs of length four were used. Experiments were run using both English and [███████████████████] For English, digraphic transposition weights were used.

$$w(i,j) = \log \left[\frac{\dfrac{f_{ij}}{N}}{(\sum_i \frac{f_{ij}}{N})(\sum_j \frac{f_{ij}}{N})} \right] = \log \left[\frac{N^{f_{ij}}}{(\sum_i f_{ij})(\sum_i f_{ij})} \right]$$

For [█████████████████████████] digraphic chained weights were used.

$$w(i,j) = \log \left[\frac{\dfrac{f_{ij}}{N}}{\sum_j \frac{f_{ij}}{N} \cdot \frac{1}{c}} \right] = \log \left[\frac{c^{f_{ij}}}{\sum_j f_{ij}} \right]$$

APPROACH #1:

All possible crib placements were located. For each place-ment, a sequence of preceding and following quadruples were scored. If a sequence of MINSPAN or more quadruples each of which scored above THRESH was found, it was printed. The next placement was then examined. More formally,

if possible crib placement is l_1, l_2, l_3, l_4

then calculate s_i=score $(l_1-i, l_2-i, l_3-i, l_4-i)$ for i=1,2,...

until s_i<THRESH

then calculate s_j=score $(l_1+j, l_2+j, l_3+j, l_4+j)$ for j=1,2,...

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

until s_j < THRESH

if max i + max j $\geq$ MINSPAN then output the quadruples just examined and their scores. Proceed to examine the next possible placement of the crib.

NOTE: Score $(a,b,c,d) = w(C(a),C(b)) + w(C(b),C(c)) + w(C(c),C(d))$
        where $C(a)$ is the cipher letter at position a.

RESULTS: Four messages in [   ] were processed.

   Message No. 1:   The cribs were placed correctly and had high
                    scores.

          2:   The correct placement wasn't found.

          3:   The correct placement was found but it had a
               low score.

          4:   The correct placement wasn't found.

Two messages in English were processed.

   Message No. 1:   The cribs were placed correctly.

          2:   The correct placement wasn't found.

APPROACH #2:

    The same scoring of quadruples was used. The sum of the
scores for SPAN quadruples was examined. The intent was to
lessen the effect of any one "bad" combination of four letters
in the vicinity of the correct placement. More formally,

$$\text{for possible placement } l_1, l_2, l_3, l_4$$
$$\text{calculate SUM} + \sum_{i=0}^{\text{SPAN}-1} \text{score} (l_1 - i, l_2 - i, l_3 - i, l_4 - i)$$

   if SUM/SPAN > THRESH   print the result

$$\text{calculate SUM} = \text{score} (l_1 + 1, l_2 + 1, l_3 + 1, l_4 + 1) + \sum_{i=0}^{\text{SPAN}-2} \text{score} (l_1 - i, l_2 - i, l_3 - i, l_4 - i)$$

   if SUM/SPAN > THRESH   print the result

             . . .

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

(continue calculating and testing the last SUM is
SPAN-1

$$SUM = \sum_{1=0} score (1_1+i, 1_2+i, 1_3+i, 1_4+i)$$

Proceed to examine the next possible placement.

RESULTS: The approach was used on message No. 3 of [   ]
[   ] It located many "good" placements (SUM>12 for
SPAN=10); however, it failed to locate the correct placement
(SUM fell between -5.06 and 1.67 for all alternatives).

CONCLUSIONS: These experiments, done for B1203, seem to indicate
crib dragging using digraphic weights is an unreliable technique
for breaking into single transposition. B12 is currently revis-
ing the weighting and threshold parameters in an effort to make
this technique work.

** **

SEEDLINGS

---The new rulings on retirement have hastened the exodus of several of our cohorts. Saying "So long" on 30 June are:

    Frederick Stires, B04
    Margaret Gohrband, B12
    Thelma Cook, B21
    Dicey Coyne, B21
    Mary Talley, B22
    Chris Christenson, B41
    Fred W. Johansen, B44
    Margaret Hickernell, B44
    Theodore Lively, B44
    Caroline Flaccus, B45
    Mary Henley, B61
    Dorothy Evans, B63

Good luck! Keep in touch! And, remember the Phoenix Society!

****

---If you're having a bit of difficulty with your AG-22 data base query and response techniques, you may find the series of programs developed by Bill Davis, B2, and catalogued on the 370 the answer to your dilemma. These programs allow the user to make specific SPECOL queries to manipulate the data base as desired.

An interesting example is the program called DF FIX, which is designed to provide a fix list by RAD using line bearings retrieved through SPECOL from the STRUM/ AG-22 data base. Routines are available which allow the user to correct identifications (RADs) and delete unusable DF modules before program fixes are attempted.

For information about other programs in his library, Bill can be reached on 5561s.

****

---MANAGERS NEEDED--WANT TO APPLY?

The American Management Association, which has sponsored conferences for women managers since 1967, says attendance at these courses has roughly doubled in the past year. "Women are hungry for management education," asserts Rosemary LeBoeuf, a program director for the Association.

Where are the hungry women in NSA? If what we are really working for is acceptance as a matter of course in being considered for and performing any job for which we have the capability, let's become qualified.

The Cryptologic Management Department of the National Cryptologic School and local universities offer programs which emphasize the issues found in most of the new management courses for women: decision making, communications,

TOP SECRET UMBRA

problem solving and group dynamics.

Here is the real challenge. Do you desire management training? Are you personally willing to invest your efforts to participate in management training? Do you know what is available and what the prerequisites are?

If your answer to the first question is no, forget it. If your answer to the second question is yes and you need answers to question three, call Helen Schmidt, ext 6101. This is the first step in getting your training requirement into the system.

---Be a WINner with WIN---

****

---B Group Language Coordinator's Office has recently published the second of a series of language aids, entitled, "Handy-Dandy 2." These aids are being compiled primarily for the many Chinese linguists in the Agency who desire to learn or maintain familiarity with terms commonly used. Many military personnel arriving at the Agency from language schools have mentioned a forgetfulness or unfamiliarity with some Chinese characters and instead of fighting their way through "dozens" of former textbooks they want something "handy."

These language aids are not intended to serve as texts, but as guides for vocabulary studies with some Chinese character exercises that should be beneficial for the serious student.

Copies of these "Handy-Dandy" aids have been provided to various B Group Offices, NCSch, incoming Chinese linguists, and to other interested personnel. Suggestions for new language aids are earnestly solicited by B02.

****

---B12's Project CALLIGRAPHY, aimed at developing a software package capable of reproducing on-line any of the several writing systems encountered in Southeast Asian communications, produced its first usable Chinese character decrypt on 16 April 73.

The idea behind this undertaking is to provide analysts of languages with non-roman alphabets the same services available to other linguists---decrypts, working aids, etc., in the native script. (See *Dragon Seeds* Vol 1, Nr 4, Sept 1972).

Being developed is a system similar to G Group's VICEROY system ▮▮▮▮▮▮▮▮▮▮▮▮ The significant difference is that VICEROY uses a fixed vector character set which makes it language specific. CALLIGRAPHY is designed for user implemented character sets and is therefore language-independent.

****

---If you would like to have a copy of Military Cryptanalytics (Callimahos and Friedman) Volumes I and/or II, please call the Cryptanalysis Department, NCSch, on 8-8025. There are a limited number of copies of both volumes available.

****

---TRANSCRIBER BONUS CLARIFIED

The Language Career Panel's 1968 edition of the "Criteria for Certification of Professional Linguists" provided for an additional 100 points under the Language Ability Criterion for "demonstrated ability to transcribe operational voice tapes" (Paragraph IIC). The Panel evolved the following policy governing the awarding of this bonus:

1. Certification as to operational transcriber ability was to be accomplished by the aspirant's supervisor by means of a memorandum to the Panel.

2. Transcriber bonus was to be awarded only in cases where it could be certified that the aspirant was or was capable of transcribing operational voice material.

3. The bonus was to be awarded only after the aspirant had passed the PQE and had satisfied all other criteria minima.

4. Where the transcriber certification pertained to non-current experience only, the Panel reserved the right to require the aspirant to demonstrate his transcriber ability by taking a specially prepared test, the forerunner of Part IIB of the present PQE format.

A number of voice transcribers in the Agency achieved their professional certification in this manner and the procedure fulfilled a much needed escape valve in the certification squeeze for these people.

With the promulgation of the Revised Criteria in June 1972, the procedures for awarding additional points for demonstrated language ability were modified. Credit on the basis of a supervisor's certification was discontinued. The Panel now grants an additional 100 points under the Language Ability Criteron for any one of the following:

a. Exceptional performance on both parts of the PQE.

b. Acceptable (passing) performance on Part I of a second language examination.

c. Acceptable (passing) performance in one additional SIGINT discipline (Part II) within the same language.

The Panel's revised Language Ability Criterion became effective upon publication (12 Jun 72). No grace period was allowed. However, the Panel recognized that some special accommodation had to be made for those aspirants who had been counting on the old bonus when they finally passed the PQE. The Panel modified its policy to continue awarding the 100 points for transcriber ability under the 1968 Criteria until 12 Jun 73 for those who had already submitted such certificates. In extending this provision, however, the Panel ruled that to qualify for the old bonus, aspirants would have to take and pass Part IIA (SIGINT Translation) of the new PQE which equates to the former Part II. Passing Part IIB (Transcriber's

option) obviously does not satisfy
the intent of the Panel's original
policy, for in allowing it the
aspirant would receive double credit
for the same thing. This point is
made here in order to clarify any
possible misunderstanding that
might arise during the overlap
period between the expiration of
the 1968 Criteria and the effective
date of the 1972 revision.

****

---Did you know that B is investi-
gating the development of a
computer system to provide on-line

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

****
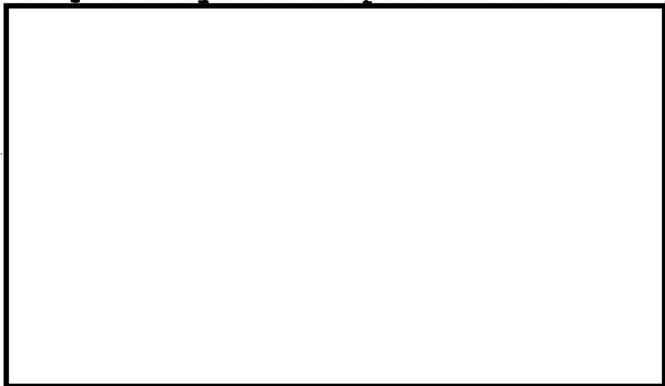
---Be sure to read Jerry Gegan's
(B12) interesting article in the
May issue of QRL to get some insight
into the problems connected with
training and utilizing military
linguists at field processing sites.

****

ATTENTION BOOKBREAKERS --

   "Collected Articles on Code
Reconstruction" is the title of
a recent NSA publication, edited
by Constance Clarke and Kay Swift
for collateral reading in the
bookbreaking course, CA-301.
Anyone wishing a copy may request
it through Betty Ames, E13,
x8025s, FANX II.

****

---Be sure to read the bulletin titled "College Training Program, Fall Semester 1973" issued by the National Cryptologic School if you're planning to take some after-hours courses next semester. To be eligible for Agency sponsorship (2/3 of your tuition and associated laboratory fees), you must

1. be a full-time (40 hour week) employee.

2. meet the admission requirements of the college or university of your choice.

3. be requesting Agency sponsorship for the first time or have maintained a C+ average in previously sponsored courses.

4. obtain the endorsement of your supervisor or office chief.

5. have no outstanding obligation from previous Agency-sponsored training.

****

---AACC at Fort Meade

Anne Arundel Community College will increase its commitment to educational service this fall by providing a full program of college courses for personnel attached to Fort Meade.

Designated in Spring 1974 a Servicemen's Opportunity College (SOC) by the American Association of community and Junior Colleges, AACC expects an enrollment at Fort Meade of approximately 2000 in study programs leading to the Associate in Arts degree.

The result of collaboration of the AAJCJ with Defense Department Educational agencies, the SOC program now involves over 100 two-year colleges throughout the nation and is coordinated to provide service personnel easy transfer of credits and continuity of curricula from one college to another.

****

---You computer buffs may wish to mark on your calendars the dates of a series of seminars being presented by Advanced Management Research Inc. on new approaches to solving difficult data processing problems.

The use of microfilm and the development and improvement of microfilm information systems will be discussed at a 3-day seminar to be held in New York City from 16 to 18 October 1973.

An intensive course in systems design and analysis will be conducted in the same locale from 24 to 26 October 1973. This seminar will discuss what is expected of the new analyst and how he can best meet the challenge.

Data base design is the subject of the seminar to be held from 28 to 30 November 1973 in Washington D.C. This course has been developed to give an analysis of the current state of the art of data base development.

ASK

THE

DRAGON

LADY

A 10 April 1973 memorandum signed by General Phillips
states, "The Management Review has indicated that we may
have some problems in our manning of linguist...billets.
I wish to examine in detail the nature of these problems
and the actions we might take to resolve them."

The Dragon Lady submits the following sentiments voiced
by some of our senior language analysts in various conver-
sations on the same subject. Opposing or supporting arguments
are solicited.

"The professional linguist at NSA who wants to remain
in language work must accept definite career limitations.
Except in the rarest instances, he cannot expect to advance
beyond a certain point as a linguist. To progress further,
he must become strictly a manager--and management is another
profession.

"That this situation exists is the fault both of higher
management and of Agency linguists themselves. Managers tend
to think of linguists as interchangeable "bodies." (After
all, "Anyone can look up words in a dictionary.") Skill
levels, experience, and capability are given only perfunctory
consideration. On the other hand, linguists often find
their work at NSA so interesting and enjoyable that they are
willing to accept, without protest, the lack of advancement
opportunities within their field."

****

~~TOP SECRET UMBRA~~

On the subject of supply and demand:

"We, because of security, are not allowed to compete in the university world; we are not even allowed to compete on an inter-agency governmental basis. Do you think that there is any real opportunity for linguists to sell their talents to the highest bidder? NSA certainly provides no opportunity for us to get together with fellow professionals of other agencies in any situation except under close official observation.

"Free enterprise for government linguists is strictly out of the question. If linguists' salaries are lower at the Library of Congress, at State, at CIA, at FBIS, don't you think it is partly because of this? Once you have worked at one of these places, no one else will touch you. We build our own little empires and never never leave them. But in how many other businesses and industries are you a <u>prisoner</u> of your profession after five years?

"And the fiction that government salaries are so much better than those of the outside world is strictly that.

"I know that many of the better universities have full professor salaries in the $30,000 to $40,000 range, which is a very rare thing in the technical, as opposed to the managerial, positions at NSA. And in my view the "pure" professor, as distinguished from the department head, provost, deans, etc., is the professional equivalent of the "pure" technician at NSA.

"What I have said is aimed at the more mundane aspect of our profession (money), but it may help to round out the picture of the linguist's professional situation at NSA."

* * * *

"When I was a GG-7, I had fantastic personal responsibility. I was responsible for developing the Agency's whole Xendian language program. Then, as a GG-13, I was reduced to counting chairs in classrooms."

* * * *

~~TOP SECRET UMBRA~~

"Languages change constantly. The skills required in language jobs take a lifetime to develop, while those required in the other disciplines are teachable in a short range of time. Language analysts are not given enough incentive to make language work a lifetime pursuit. I'm not sure where the stopping point is. In the middle ranges (GG-7 to GG-13), there is a reasonable career. But, beyond that, it's questionable if enough incentive exists to keep people in the field. And then, we're stingy with our training. There is no overall long range training program in terms of the needs of the Agency and the needs and capabilities of the person.

****

"As long as promotion above a certain level is on the basis of management, there will always be a shortage of technicians. This is true for other disciplines, too. Not taking anything away from management, but there _are_ other skills that are just as critical to our mission."

****

"It is wisdom to know others;
"It is enlightenment to know one's self."

---Lao Tzu

```
        T  H  E  W  I  S  D  O  M  O  F  T  H  E  C  H  I  N  E  S  E  S  A  G  E
       23 11  4 25 14 20  3 18 16 19  9 24 12  5  2 13 15 17  6 21  7 22  1 10  8

  1    T  O  M  E  N  D  B  U  T  T  F  A  I  L  X  E  Q  U  I  T  N  C  E  R  I
  2    C  I  U  S  O  H  E  R  E  W  B  Y  T  H  E  Y  X  C  L  E  G  H  T  E  O
  3    N  E  D  O  C  A  S  N  O  D  P  E  O  P  L  A  N  G  O  V  U  S  N  E  S
  4    T  R  I  N  E  I  V  I  N  E  E  X  X  M  E  E  R  N  M  E  S  A  N  D  C
  5    W  A  S  S  A  R  I  G  H  T  N  C  I  U  S  N  T  X  C  O  O  N  S  C  I
  6    C  R  E  D  X  O  F  K  I  N  H  E  L  D  T  O  P  E  R  A  E  N  C  E  W
  7    X  I  T  H  A  G  S  X  T  H  H  A  T  T  H  T  I  O  N  F  E  R  E  I  N
  8    D  C  O  M  E  E  U  N  F  I  E  G  E  N  E  O  R  P  U  B  N  A  T  E  I
  9    D  O  W  N  F  T  A  M  O  N  R  A  L  W  E  L  I  C  I  M  N  M  A  N  X
 10    R  O  M  R  E  G  W  H  O  M  L  F  A  R  E  P  R  O  V  E  X  T  H  E  I
 11    M  O  T  E  A  S  H  O  U  L  O  F  T  H  E  M  E  N  T  X  M  P  L  I  C
 12    N  T  I  Q  U  D  B  E  R  E  P  E  O  P  L  A  N  D  L  I  A  T  I  O  N
 13    I  T  Y  X  X  M  O  V  E  D  E  W  A  S  A  B  E  R  T  Y  B  E  I  N  G
 14    R  O  Y  A  L  B  Y  T  H  E  B  O  V  E  A  O  F  C  O  M  T  H  A  T  M
 15    G  O  V  E  R  N  R  E  Q  U  L  L  E  L  S  M  E  R  C  E  O  R  A  L  L
 16    N  M  E  N  T  A  L  S  O  R  E  X  X  H  I  X  X  H  E  H  A  W  I  S  O
 17    W  A  S  A  N  X  S  H  O  U  S  V  O  I  C  E  L  D  T  H  N  E  W  I  T
 18    I  N  S  T  I  L  D  T  H  A  E  W  A  S  U  A  T  B  E  N  H  C  R  E  A
 19    T  U  T  I  O  T  P  R  O  C  P  L  I  F  T  E  V  O  L  E  T  I  O  N  X
 20    N  O  F  G  O  E  D  U  R  E  E  D  F  O  R
```

Solution to March trans-
position Puzzle.

Answers to Crypto-Scramble: Cryptoanswer:

    Delta I.C.   ANAGRAM
    Monograph
    Average I.C.
    Sigmage
    Tables

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 thereaftre. 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.

PEGGY BARNHILL joined NSA in 1966 after graduating from Marywood
College with a degree in Social Studies. While a participant
in the Special Research Intern program, she worked in various
areas throughout the Agency. Upon completion of that program,
she was assigned to B42, where she has been deeply involved
in development of the software for processing AG-22 data.
She is professionalized in both Special Research and Data
Systems career fields.

DR. MARTHA A. (MARTI) BRANSTAD, P1, entered NSA as a Crypto-Math
intern in 1971. She has had tours in R, C, and B. It was
while touring B12 that she isolated several "bugs" in the
370/STETHOSCOPE, a series of C/A diagnostic programs. This
discovery led to her present undertaking--that of revamping
and debugging the whole RAPIDS (general utility program)
package. Dr. Branstad's background includes a PhD awarded
by Iowa State University, where she briefly served as
Assistant Professor of Computer Science. Even now her ties
to the academic world are not completely severed, for after
hours she teaches at the University College of the University
of Maryland.

RODNEY FORBES majored in English at Notre Dame and Ohio State,
where he received his M.A. in 1951. After a stretch in the
Army, he kicked around graduate school at Ohio State for a
while, studying and teaching, before joining NSA in 1957. He
has spent almost his whole Agency career in B Group, having

worked on the [ ] problem and the CHICOM [ ]
and Development problems. But he has spent more time on the
CHICOM [ ] where he is now serving another
tour. With Sally Keil, he published a long TSR (B43 #1-71)
on the same subject as his Dragon Seeds article.

WILLIAM D. GERHARD has been with NSA since 1952 except for a
two-year period from 1962 to 1964, when he worked for the
Science Information Office of the National Science Founda-
tion. At NSA, he has divided his time between G and B
Groups--in G as a linguist, cryptanalyst, and reporter and
in B as a member of the B6 Operations Staff (1964-65) and
the B6 Technical Support Division (T/A, C/A, and machine
support) from 1965 to 1967. Since then, he has headed a
small NSA/SCA team chartered by DIRNSA to document the U.S.
cryptologic involvement in Southeast Asia. Bill received
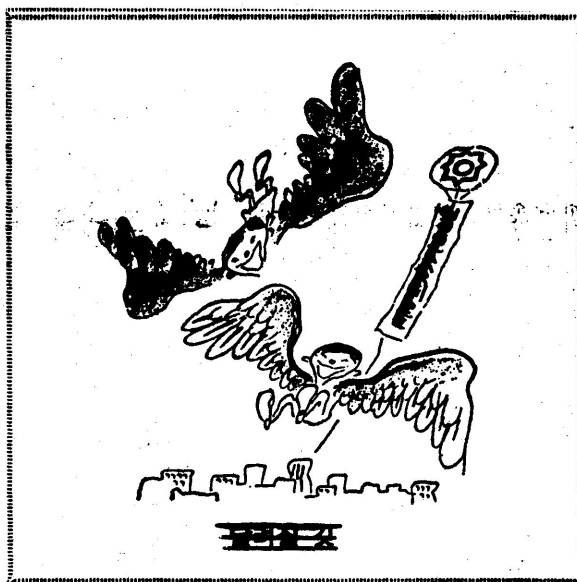his education at Indiana University, which granted him B.A.
and M.A. degrees.

BEE KENNARD, P2221, graduated from the University of Texas with
a B.A. in History and English. For seven years she served
as an intelligence analyst with G2, U.S. Forces in Austria.
From 1967 to 1971 she worked with the B2223 collocated
information support group as the senior analyst on the Viet-
nam Military problem. Currently, she is a "retired war
correspondent" and author-in-residence.

MARY ANN LASLO, B432, was graduated from Rosary Hill College,
Buffalo, New York, in 1965, receiving a B.A. degree in
Mathematics. She came to NSA in 1966 and entered the C/A
Intern Program, which provided opportunities to work in
A55, B45, G41, and G42. She received her certification
as a mathematician in 1970 and as a cryptanalyst in 1973;
and she has completed several requirements leading to
certification as a crypto-mathematician. Since 1969,
Mrs. Laslo has been assigned to B432, where she does
independent cryptanalutic research on the Peoples Republic
of China [ ] and functions as a consultant
in mathematics and statistics at Division level.

Doc ID: 6708422

保密

it's classified!!