~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

VOLUME I NUMBER I
AUGUST 1974

Classified by DIRNSA (NSAM 123-2)
Exempt from GDS, EO 11652, Cat. 2.
Declas Date Cannot Be Determined

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

P.L. 86-36

A LETTER OF INTRODUCTION

This is CRYPTOLOG -- a new vehicle for the interchange of ideas on technical subjects in Operations.

Operations is a large organization; the skills and talents on which we depend are many, our workings widely scattered and often sequestered in compartments. These conditions argue for special efforts to keep us in touch with each other and with new problems as they arise and new solutions as they are developed.

In the past this need has been partially met by a number of small specialized magazines, some keyed to a given sector of Operations (as Dragonseeds to B Group, Keyword to G) and some to subject matter (as QRL to language and Command to traffic analysis and special research). Not all areas and disciplines were thus represented, however, and distribution of the existing vehicles was limited.

It is to improve this situation that CRYPTOLOG, combining the resources of the above-mentioned vehicles, has been established. I count on it to provide all the good effects of its predecessor publications, plus additional ones. As a monthly it can be more responsive than the quarterlies and bi-monthlies it replaces. Because it is Operations-wide it can embrace all our disciplines and address all our people. Its classification, up to and including Top Secret Codeword, permits discussion of very specific subjects in the cryptologic sphere, and its level of informal exchange invites short articles and letters on any subject.

To be successful, CRYPTOLOG must reflect current operational topics in a way that interests you and others. I hope that you will want to read it and will help to write it.
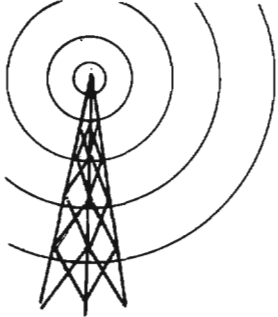
HERBERT E. WOLFF
Major General, U.S. Army
Deputy Director, Operations
NSA, CSS

WHAT IS A COLLECTOR?

by [ ]

If you have looked at the masthead of this magazine you will have seen that the various members of the editorial board represent different disciplines. When seen in life, nobody has trouble distinguishing among these disciplines: everyone knows that traffic analysts are clear-eyed, clean-limbed people who draw meticulously neat--if arcane-- squares and circles on paper, and that cryppies are two-headed people who tend to twitch. The machine people are those pale ones who inhabit, like troglodytes, the bowels of the basement. Collectors are--uh--aren't they the can-clangers who come around three times a week with a truck?

Collectors are a strange breed. Outside of the National Security Agency and a few other agencies with which we deal it would be a hopeless undertaking to try to explain them. It will not be easy explaining them to people who should know.

Personnel assigned to NSA in billets identified with a Career Occupational Specialty Code in the 1600 series are collectors. That is one way to identify them, but not a very effective way. Agency employees don't have their COSC's stamped on their foreheads. Let's look at this another way. What do collectors do? Well, you know those pieces of traffic that traffic analysts analyze? They were collected by collectors. In fact, a number of collectors working in concert got the analyst his piece of traffic.

Somebody downtown decided that we could not go another minute without finding out what the Zendian Army's 279th Underground Balloon Battalion was up to. Then somebody important in NSA, in V5 as a matter of fact, agreed that this was a valid requirement, translated this demand into NSA-ese and tasked one of (presumably the appropriate) elements in DDO. (When translated, the task becomes, "Find out what the 279th Underground Balloon Battalion of the Zendian Army is up to." Actually, by this time it will be known as the 279th UBB, and as it is a pronounceable acronym, it will be pronounced.[1]

The neophyte who has to ask "What's UBB?" may receive a polite if patronizing explanation. More likely, however, the response will be, "Not much, what's ubb with you?")

Enter the first collector, the collection manager in the office of primary concern--in this case, whichever office is responsible for Zendia. He will say something like, "Gee whiz![2] I already have 47 cases on each position I own and the bottom 45 in the priorder don't get heard now!" (The cases are listed in priority order, and having too many cases on too few positions is a chronic problem.) To assign this new task in such a way that it may have a chance of being heard, he may take his entire mission apart, shuffle it around and rewrite every assignment. He has a good idea of what may be heard where, what kind of equipment he needs to do which jobs at which sites, what book of rules he has to consult to render a simple requirement incomprehensible to anybody who doesn't own a copy of the same book of rules, and what he has available to do the job with. Additionally, it serves him well to know what other managers have and what they need, in case a trade is necessary. Finally, he has to know where he can get help if he has to have it in order to satisfy the requirement.

After the details are worked out and the task is converted to a Collection Control Message (CONMSG) or a Signals Collection Objectives List (SCOL) or whatever happens to be currently fashionable, it goes to the site or sites where the actual collection will take place. Another collector receives the task and tries to translate it back to English. His title may vary from station to station, service to service, but his function is to manage the collection resources at his station. He is intimately aware of the capabilities in his station, he knows what talent is available, what conditions his resources are in, where he can cram the mission in--specific instructions from the manager at NSA notwithstanding--and, often, what rules he has to break or instructions he has to ignore in order to get the job done. (Incidentally, we at Fort Meade have absolutely no idea that he is breaking rules or ignoring instructions in order to get the traffic to us--as long as he gets it to us.)

Now the mission is in the hands of the operator. His is the real collection function. He finds the signal that the Zendian UBB 279 is using to convey whatever it is they are conveying, he records in some way the signal itself and information about it. That is, if it is a Morse signal, he copies what the Zendians are saying to each other. When the signal is weak and atmospheric conditions are not conducive to facile copying, the Morse operator sometimes mutters "Tut!" or even "Darn!"

In addition to copying the signal, he records on his logs such information as the frequency it is operating on, the time it is active and other ancillary information from which predictions may be made about future activity.

If the signal is non-Morse the operator must determine what the nature of it is and manipulate machinery to copy it, but the principle is the same.

The collectors in all of the steps, from the operator on the position to the exalted manager in his luxurious Fort Meade office, must also know something about the other disciplines in order to do their jobs effectively. They ought to know what kind of information is important to the traffic analyst, in order to be alert for that kind of information when it appears. They have to be aware that indicators for the cryptanalysts may appear in traffic and that it is important to collect them--and helpful, sometimes, to highlight them.[3] The collectors at the management levels have to be familiar with the needs and wants of the other disciplines in order to meet them or to anticipate them when writing and assigning tasks. They should also constantly remain aware that every collection success creates a processing problem. Hence the collector must be aware of and should be sympathetic to the problems of the other disciplines.

This is a vastly oversimplified account. This writer is a collector, and at one time or another each of those activities was his job. This article has not gone into any of the details of a collector's job. It was intentionally designed to be a brief introduction to a relatively little-known discipline, but one without which the other disciplines would have no reason to exist.

Another motive for this article was to throw down a gage. Many readers are going to say, "I could write rings around this guy." Anyone who can, ought to. Even if you can't write rings around this guy, you probably have something to contribute. Write an article on some aspect of Collection, or tell us about an experience you have had as a collector or with collectors, and whip it on the editors.

* * * * * * *

1. Acronyms don't have to be pronounceable to be pronounced. Take, for example, "Discus" satellites (DSCS), "Flare-9" antennas (AN/FLR-9) and "Angry-9" radios (AN/GRC-9).

2. Collectors are often given to strong language. Some expletives used in this article have been modified to protect more sensitive personnel.

3. Some Morse operators are instructed, for example, that unless the preamble and first five groups of text are copied, the rest of the message is not even worth taking.

(CONFIDENTIAL)

CLIP OUT AND MAIL TODAY
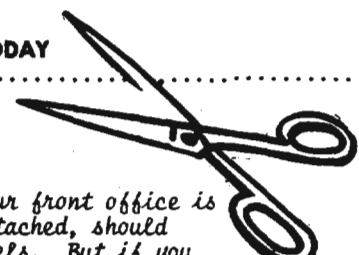
SUBSCRIPTION COUPON

If our circulation department is doing its stuff and your front office is doing its stuff, a copy of CRYPTOLOG, with buck-slip attached, should reach you every month through your organizational channels. But if you would like to have a copy mailed direct to you in your own name, fill in this coupon--or any old slip of paper--put it in a shotgun envelope and send it to CRYPTOLOG, P1.

(Name) _____

(Organization) _____ (Secure telephone) _____

TDB ☉ THE TEXTA DATA BASE
by William J. Jackson, P14

TEXTA means Technical Extracts of Traffic Analysis. A system of recording and maintaining a data base of technical information on communications targets, it was instituted in 1946 by agreement among NSA,
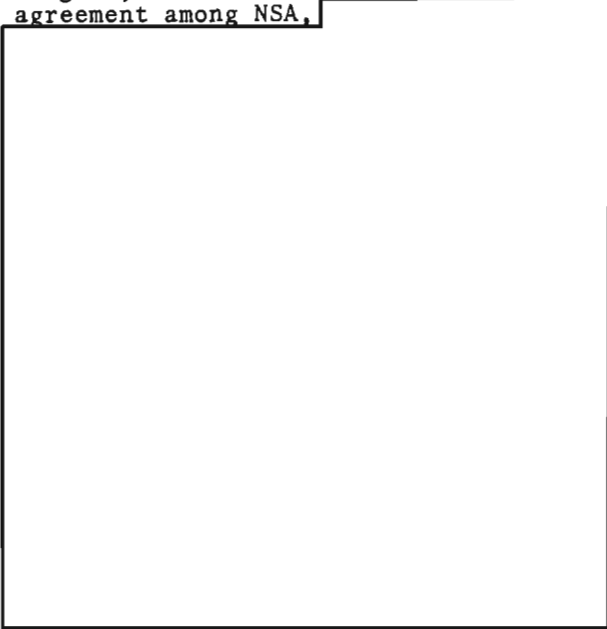
In recognition of the problems arising from the variety of TEXTA-related systems, Major General Herbert E. Wolff, Deputy Director, Operations, NSA/CSS, has directed that a world-wide common TEXTA data base, to be known as the TDB, be established, to comprise one technical file which will embrace both TEXTA and specialized files, meet field needs, simplify feedback operations, and be compatible with the activities of collaborating centers. He has designated P1 as overall management authority for the development and initiation of the TDB; Mr. William Lutwiniak, Chief P1, has named Mr. C. G. Garofalo, Chief P14, as the project manager. Assisting Mr. Garofalo are sub-project managers named by Operations Groups A, B, C, G, V, and W. This committee is meeting periodically to develop and establish the TDB. Members are ascertaining the ideal data base requirements of each using organization, identifying common elements in these requirements, and determining what additional elements might be needed. Considered in the planning is the rectifying of factors which caused the variety of TEXTA-related systems to come into existence.
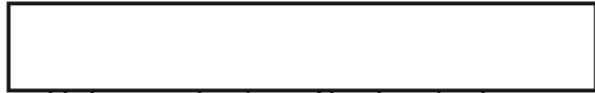
will be involved in the final stages of the development of the TDB. Upon agreement of all concerned, an ideal TDB format will be developed, after which C Group will be requested to devise and establish flexible machine processing systems to handle all present and anticipated TDB requirements. Following initial implementation, V3 will assume operational control of the system.

(SECRET HVCCO)

EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

==

WHAT SHOULD YOU EXPECT?
or The Analysis of Cryptanalysts

BY

You are a manager among whose newly acquired responsibilities is the production of intelligence information from encrypted messages of a SIGINT target. Your personal background is firmly in traffic analysis and reporting, and you have always felt that cryptanalysis was an esoteric art that an outsider could not really appreciate. Now you must sit in judgment of people and operations in that "foreign" field. What should you expect of a crypt effort? More pertinently, what should you expect of the cryppies involved in it? If your deputy is an experienced, professional cryptanalyst, you have some breathing space, but the responsibility is still yours. Here are some thoughts from one professional cryptanalyst and erstwhile manager which may help.

The good crypt effort, whether manned by one or one hundred people, is marked by a "professional" outlook. Webster's defines pro-fessional as, among other things, "manifesting fine artistry or workmanship based on sound knowledge and conscientiousness." The definition covers the product, the methods used to produce it, and the fundamental principles from which those methods proceed. Principles and methods imply order, and the good crypt effort is orderly. That is not to say the desks and papers are neat; it is to say there is intellectual order in the attack on the target problem. For the members of the group characteristically use the scientific method of systematic pursuit of knowledge, yet--and we might consider the "fine artistry" part of the definition--they are flexible enough to allow for and to profit from the intuitive leaps that sometimes bring solutions. The lucky guess, the shot in the dark have their place, closely tied to the "surprise" and "rational behaviour" I. J. Good speaks of in the introduction to his Standard Reagents and Diagnostician's Dictionary.

Another professional attribute of both the crypt group and its members is thoroughness. Whether its mission is initial diagnosis of a large or small body of encrypted messages or the exploitation of traffic in solved systems or both, the crypt effort covers all aspects of the problem according to a reasoned plan established in the light of all the information, all the material, and all the resources available for the job.

As with other scientific professions, the good crypt effort is well documented. The Technical SIGINT Report, the SIGINT Support Report, The Technical Journal article, the Informal Technical Notes, the Technical Support Letters all put pertinent information on the record and invite evaluation and response from other members of the profession. Producing one's own publications and profiting from those of others are indispensable to complete, professional cryptanalytic operations.

Now that we agree on the characteristics of a good crypt effort, you as the manager still have to measure yours against the standard. Even without more than a superficial knowledge of the ins and outs of crypt, you can gauge your group's status with some reliability. Consider the characteristics. Is there a long-term goal? Are there intermediate stages along the way? Do the members of the group know what they are? Does the group as a whole agree on a single goal or a single set of goals? Can the group leader describe these goals to you so that you can understand them? Do the group and its members know how they will try to get to the goal? Again, can the leader explain the routes or methods to you so that you can understand? Have they alternative methods in reserve in case the first ones don't work? Is there contingency planning? Does the group consider the whole problem or only that portion that comes readily to hand? All these points have to do with order and method; they presuppose knowledge and skills belonging to the profession of cryptanalysis.

The second characteristic, thoroughness, applies to the order and method; it also applies to the execution of the chosen methods of getting to the end result which lies somewhere along the path of diagnosis, solution, exploitation. Does the group collect all the available traffic? All the pertinent traffic analysis information? Collateral? Does it study all the material and information gathered? Does it know or find out or write or request and use appropriate computer programs? Does it consult experts in the field? Does it study reports on what has been done in the past against the same target? Against the same type of cryptosystem?

It comes last in the list of characteristics and it all too often comes last to mind if it surfaces at all--documentation. Yet it is an integral part of the professional and scientific effort in cryptanalysis as in any other technical discipline. You, the manager, should expect that the procedures and results will be put on the record. Does at least the group leader keep a technical diary? Does your group report in writing? Does it publish technical reports? Does it think that only successes are reportable? Does it report, for the record, procedures developed or adapted, with information on the material the procedures were applied to, and the outcome of the application, failure or success, in whole or in part? Are the reports well written? Can you understand them or at least grasp the essentials of what was done and why? Do the reports published by your crypt group provoke questions, suggestions, refutations, visits, or telephone calls from other cryptanalysts or other crypt organizations?

Having looked at the effort, let's consider the individual. The same features that mark the good crypt effort mark the activities of the good cryptanalyst. Only the scale is smaller, and the personal attributes of the individuals vary from one to another. Aside from the specific training and experience one would need for your problem, there are some generalities about the "professional" cryptanalyst (not necessarily so certified by the Career Panel).

Mature, responsible, self-reliant, forward-looking, optimistic--all the trite laudatory adjectives--mark the good analyst. Add common sense and sound pragmatic judgment and a willingness to share knowledge with others, and you come closer to the ideal. He may be a "loner" by inclination and may be more valuable to the effort working that way, but he always knows how his problem dovetails with other problems or with other facets of the same problem. He knows and subscribes to the set goals of the group and, indeed, of the Agency.

The good cryptanalyst keeps up with developments. He reads technical publications, participates in professional assemblies and conferences; he seeks advanced training to sharpen crypt skills and to increase his knowledge of related fields. He talks to other analysts and learns from those he talks to. He finds out what is going on in related fields. He does not retire to his own snug corner and let the rest of the SIGINT world pass by.

· The good cryptanalyst is intellectually alive. He keeps learning and keeps trying to relate what he learns to the problem he is dealing with. He can tell you what he is doing and why, and he wants to. He keeps on working and never completely abandons hope of eventual success, but he knows when the law of diminishing returns becomes operative and is willing to call a halt. He documents what he has done and what he thinks ought to be done if the propitious time ever arrives. He prepares for the future-- his own and the problem's.

To judge the cryptanalyst and his work, the non-cryptanalyst manager should look for knowledge and commitment to goals, both organizational and personal; for thoroughness; for documentation of work and outcome; for order in materials and methods. The questions to ask are really the same as for judging the whole effort. In addition, look for initiative, imagination, innovation, and enthusiasm tempered by practical good judgment about potential results. Beware the pitfall of judging the capability and performance of the individual primarily on the basis of the number of systems solved or messages read--there are all kinds of systems and all kinds of messages.

The documentation of the crypt effort of whatever size can give you insight into both the group's and the individual's operations. Technical reports, published and unpublished, formal or informal, can help you evaluate the effort, its directions, and its prospects as well as its people. Good documentation shows that the cryptanalyst is looking beyond his own desk--to other SIGINT fields and to the future.

To judge crypt documentation, read the reports. Do they cover the whole problem or, if they cover only part of it, do they describe how the part fits into the whole? Do they fit in with what you know from other sources? Are they written while the information is still fresh in the author's mind? Are they convincing? Do you understand at least the general outline of the problem, the work, and the results? In other words, are reports written? Are they well written? Will they be useful for the next crypt attack on the same problem or on similar problems of the same or another target now or in the future?

The cryppie knows he has reached a solution when the system "reads." You, the manager, have no such definite measure in evaluating a crypt effort. Perhaps these few ideas can provide a starting point to help you arrive at a reliable judgment about this part of your responsibilities.

EO 1.4.(c)
P.L. 86-36

SECRET

A SPOT BY ANY OTHER NAME by VERA R. FILBY, E12

When things or situations or the contexts in which they exist change but our words for them do not, it may be some time before we perceive the disparity between our understanding of the words and the reality they represent. Such a disparity appears to be affecting names for certain SIGINT reporting vehicles.

Take the term electrigram. The word was invented in the mid-1960's to distinguish between reports of current events issued electrically soon after the events happened or could be recognized, and routine, recurring reports, such as daily and other summaries, which were issued electrically. Instructions celebrated the newness of the term by showing it in caps: ELECTRIGRAM. It soon acquired the nickname E-GRAM and eventually tended to lose its majuscule status. It was defined as "a vehicle for publishing information that does not meet the criteria for SPOT Reporting....but which is of significance and/or urgency requiring electrical dissemination."

Distribution instructions brought out a further distinction in that electrigrams, unlike spots, were not
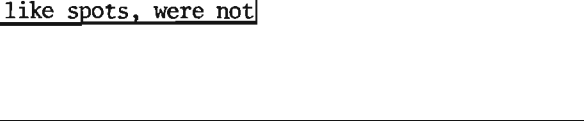
Thus the meaning of the term was clearly defined, and it made sense in the context of SIGINT reporting--until a year or two ago. But changes resulting from, among other things, automation, security, and economy, have altered the context situation. Now, for example, many reports are issued electrically which formerly would have been issued in hard copy only. These may be reports of information a week, a month, or six months or more old, information not exploitable when current, or not useful or recognized as useful at the time, or of limited priority but still reportable. The question now arises: When such a report is issued, is it an electrigram?

The problem is not as trivial as it may seem. People need to understand what words mean, and there must be common understanding of terms and their significance between writer and reader, because that means common understanding between analyst/reporter and user.

Consider the spot report. Some reporting units and some instructions have set time limits of 30 minutes or even 15 minutes from time of recognition of spot information to time of release. But urgent and important information may be quite complex. It may require extensive processing and analysis. If it takes a day, or two, or more, for processing, coordination, and release, but must go to a spot distribution because of content, is it still a spot? Instructions define spot report information as "highly significant, perishable SIGINT" and require that spot reports be labeled as such. They also require a precedence of PRIORITY or higher. But current telecommunications system regulations call for a maximum handling time for PRIORITY precedence of three hours; so what is the point of a 30-minute reporting requirement? At present (Spring 1974), with the degree of automation achieved over the past two years, average system handling time for PRIORITY is about seven minutes, but actual delivery time for both ROUTINE and PRIORITY is about two and a half hours, for IMMEDIATE about one hour, and for FLASH about 10 to 15 minutes.

Sometimes a brief summary of complicated facts can be issued as a spot with the details in a follow-up, and this may be a useful device for getting out urgent but complex information. It is less useful for information less urgent but still requiring spot distribution, since it means that readers must refer to two documents instead of one to get the story.

Because of distribution requirements, there has been a tendency lately to put a SPOT REPORT label on items which do not meet the definition of "spot" as urgent and perishable but may even be wrap-ups or periodic summaries of a continuing situation. A puzzled user who was asked recently about a rather relaxed reaction to information in a spot report responded plaintively, "But we don't know what a spot report is!"

Is it any wonder?

And so a process of rethinking and redefining is now under way. Would you like to help? Any ideas? Try defining:

An electrigram is.....

A spot report is.....

SECRET

THE NEW TRAFFIC ANALYSIS GLOSSARY by P14

"Glossary" is defined as a collection of terms limited to a special area of knowledge; it derives from the Latin glossa, which refers to an unusual word requiring explanation. Since the SIGINT business includes several such areas, each of which makes use of many such words, and since its successful pursuit depends on the ability of its organizational elements to intercommunicate with precise understanding of meaning, SIGINT glossaries are a definite and practical necessity. Nevertheless, only during the past year has there been a formally directed PROD effort, under USSID 412, to develop and publish a complete, authoritative, and official glossary for each of the special technical fields peculiar to SIGINT, coordinated with and agreed upon by all using operational elements and, in some instances, second parties. Earlier, some glossaries, both specialized and general, had been published, but, with one exception, without having undergone a rigorous developmental treatment throughout Operations and without having acquired second-party agreement. These included a general glossary prepared by the U.S. Army Security Agency in 1947, a traffic analysis glossary published by NSA in 1954 (NSA Interim Report #168-54), a glossary contained in the Radio Traffic Analysis Manuals of 1955 and 1964, and, in three editions, the Basic Cryptologic Glossary, the latest dated June 1971. The exception referred to above is the Combined Glossary of Traffic Analysis Terminology, published in January 1958 by NSA, which was thoroughly coordinated throughout PROD and with second parties (the latter indicated by the term "Combined").

After the Combined Glossary was issued, a decision was made that no further glossaries would be published by PROD--that hereafter they would be the responsibility of the then Office of Training. As one result, PROD personnel who had been concerned with the Combined Glossary and who had intended to keep it updated were discouraged from so doing. Finally, in 1964 the Office of Training published an all-inclusive glossary, called the Basic Cryptologic Glossary. It included some terms used in traffic analytics, but it did not adequately or accurately fulfill PROD needs--many TA terms were omitted and some were changed from the 1958 Combined Glossary without proper coordination either with NSA elements which were operationally concerned or with second parties. Also, the Combined Glossary contained Codeword information, while the Basic Cryptologic Glossary was limited to Confidential material. Thus, two glossaries containing differing terminology and spelling were extant, leading the British to comment that "only NSA could afford the luxury of two glossaries," and, along with most of the knowledgeable NSA traffic analysts, to continue to use the Combined Glossary while ignoring the 1964 publication, at least with regard to TA terms. Later editions of the Basic Cryptologic Glossary evidenced no significant improvement as far as TA was concerned, as there was little input from and no formal coordination with NSA operational personnel and second parties.

In recognition of the somewhat confused glossary situation and the need for the development of definitive and authoritative terminology, not only for traffic analysis but for the other SIGINT disciplines, USSID 412, SIGINT Terminology, was promulgated, on 1 February 1973. This USSID established the program for standardizing terminology used throughout the U.S. SIGINT System to direct, manage, and support SIGINT operations. As part of the program, terminology panels are authorized to be established to develop standard definitions for terms required in the specialized areas of SIGINT operation. The USSID also designates the NSA Data Standards Center (NDSC) as having overall responsibility for the issuance of the respective glossaries, and makes it responsible for maintaining a complete SIGINT Terminology Data Base and for making the base, in the form of machine printouts,

P.L. 86-36

SECRET

available to authorized users, principally the terminology panels.

Under the authority of USSID 412, and with operational terms of reference agreed upon between P14 (Traffic Analysis) and P13 (in which the NDSC is located), the Traffic Analysis Terminology Panel (TATP) has been established to develop the Traffic Analysis Glossary. Under the chairmanship of Mrs. Gloria Chiles, of P14, the TATP consists of representatives of A, B, C, G, W, E, and P14, appointed by the chiefs of those organizations. Three senior cryptologists, Messrs. C. G. Garofalo, Chief P14, Robert [   ] Chief P13D, and Donald Borrmann, D/Chief V, act as advisors to the TATP.

As the initial step in the development of the TA Glossary, the NDSC made available to the TATP the printout of a terminology data base consisting of thirteen technical glossaries containing a total of 4,641 unique items presumed to have a possible relationship to traffic analytics. (The TATP found that many of these items had a variety of definitions, some as many as thirteen-- a different one in each of the contributing glossaries.) The first task of the TATP was to sift through the list of terms to identify those which could be of concern to the field of traffic analytics and which therefore would warrant further consideration. (This process, although at first glance a simple one, was complicated by the overlapping and intimate relationship of traffic analysis and other special fields, such as cryptanalysis, collection, signal analysis, data systems, etc. The difficulty apparently arises from a lack of precise definition of the field of traffic analytics - this problem is being studied by the TATP.) In addition to using this list, the TATP selected potential terms for study from a variety of operational publications, such as TECHINS, USSID's, working aids, Technical SIGINT Reports, etc. The sifting and selection process resulted in the TATP designating about 1500 terms for detailed study and possible inclusion in the TA Glossary; this study is now in progress. The terms have been grouped into two general divisions- one by subject matter and the other, those terms that remain, alphabetically. In addition, each term has

been categorized as follows:

Category 1: terms of primary concern in traffic analytics, which will be defined and included in the Glossary.

Category 2: terms of secondary concern in traffic analytics, which will be included in the Glossary but defined by other panels.

Category 3: terms determined to be of no concern in traffic analytics, which will not be included in the Glossary.

Category 4: terms to be included in the Glossary as cross references.

Subject-matter groupings consist of terms relating to a particular area of study in traffic analytics, such as callsigns, addresses, procedure, etc. Considering related terms together results both in finding and devising new terms and in eliminating some that are duplicative or unnecessary. For example, in the address grouping, 182 terms were considered and eventually reduced to less that 100. Also, in this group, a new term was created-- "coverterm"--as a generic term which includes "covername," "covernumber," and "coverword." Consolidation of terms was also effected--e.g., "weather station identifier" becomes the generic term, and "indicative," "station identifier" and "station number" are cross-referenced to the generic term by the statement "same as weather station identifier." Correspondingly, included in the definition for the generic term is the statement "synonymous with indicative, station identifier, and station number."

In its operation, the TATP establishes an agenda consisting of a list of terms to be discussed at each weekly meeting. In preparation for the meeting the panel members research assigned terms by examining technical documents and dictionaries, determining their use in operational elements, reviewing previous definitions, obtaining opinions from senior analysts, etc. Thus prepared, the panel members in open discussion at the weekly meetings attempt to arrive at a standard definition for each term. At the time of this writing, the TATP has established definitions for terms beginning with A through H, as well as for the subject-matter groupings for addresses and for communications structure and operations.

SECRET

When the definitions for all terms have been completed by the TATP they will be arranged in prescribed draft format as Annex D to USSID 412, which will be forwarded by P1 to USSID representatives in the operational elements for concurrence and distribution requirements. Concurrently, the draft, which is scheduled for completion in December 1974, will be coordinated by P14 with second parties through the existing TEXTA Working Party, of which Mr. C. G. Garofalo, Chief P14, is chairman. After completion of coordination and any required substantive revisions by the TATP, a final draft will be prepared by the NDSC for final coordination by P13 with the SCA's and second parties and eventual reproduction and distribution. Although the Glossary will be part of USSID 412 for record purposes, it is planned that it will be issued as a separate document physically, principally for ease of reference and to facilitiate distribution and use by second parties.

Publication and use of this Glossary, and eventually of those in the other specialized fields, should make for a clearer understanding in SIGINT matters among all those concerned, and thus improve the effectiveness and efficiency of their efforts.

(SECRET HVCCO)

---

*P*UZZLE 1

*A*s if the SIGINT business weren't puzzle enough, some people like to make up their own riddles and inflict them on their friends. A simple form of puzzle (which also makes a great game for children on long trips) is the stinky-pinky, in which the answer must be given in a pair of rhyming words of a stated number of syllables. In the list below, for example, all-out offensive breaks out to large charge, carefree captain to chipper skipper, and so on. While you are waiting for that call to be returned, try your hand at these.

1 syllable:
- All-out offensive
- Intoxicated agent
- Blue dossier
- Taped speech
- Polished Pole

2 syllables:
- Carefree captain
- Corrugated film
- Smaller soldier
- Facsimile messages
- Beatnik codebreaker
- Error in an epitaph
- 30-year cryptanalyst
- Poor intercept

3 syllables:
- Evil emissary
- Searching examination
- Sadat loses cool!
- Cleverer calculator
- Future goal

4 syllables:
- Deserted city
- German swimmer
- Chic Japanese

5 syllables:
- Polysyllabic ragamuffin
- Central American underground

BLAH BLAH BLAH

OH, FUDGE!!

Ach, du lieber!!

ANSWERS ON PAGE 20

THE LANGUAGE OF BEISBOL IN EVERYDAY TALK

by [ ] P16
& Ramón Santiago-Ortiz, G643

P.L. 86-36

WHEN we say that baseball is an "American" game, the reference is usually to the United States, but the sport is played and loved in Latin America as well. It has even affected their language and terms that originated on the diamond are now a part of everyday conversation in Spanish as they are in English—-compare "he's 'way off base," or "What's the pitch?" or "I really struck out on that deal!" An article in the Cuban magazine BOHEMIA collected about 35 such expressions. We have arranged them alphabetically, run the original BOHEMIA entries (as in the original, without written accents, in full capitals, etc), and supplied a rather free English translation.

The English words in parentheses on the Spanish side were in the original. The English words in square brackets are more-or-less literal translations of the capitalized Spanish (the baseball term); the remainder of the English entry consists of comment and explanation of the Spanish, rather than being just a translation of it.

AL BAO (bound).— Que nos llega fácilmente: sin problemas, a las manos.

[on the rebound, on the bounce] no sweat!, very easy, like taking candy from a baby.

¡AZUCAR!— (así bautizó el estrai un narrador deportivo).— Sublimación del piropo.

[sugar; a term invented by a sportscaster to refer to a strike] the highest form of compliment. (A whole article could be written about that word PIROPO, which is usually restricted to complimentary remarks made to and about pretty girls. Note also that word ESTRAI, strike, which we'll see again in ME TIENEN DOS ESTRAI Y PELEADO CON EL AMPAYA later in this article.)

BOTO LA PELOTA.—(jonrón).—Hizo algo en grande; óptimo o pésimo.

[he knocked the ball out of sight for a home run] He went all the way; whatever he did (good or bad), he did it in a big way; no halfway measures with him!

CERO CARRERA, CERO HIT, CERO ERROR.— Nada de nada, no de esa obediente materia prima ("pues de ella fue la humanidad creada") sino la equivalente a una cifra cero sin orillas. El elocuentísimo "nico..."

[no hits, no runs, no errors] a real nothing, a total nonentity. (Sometimes the word HIT is spelled JIT.)

COGIENDO ROLE (rolling).—Rascabucheando, viviendo un cuadro.

[catching a rolling ball, fielding a grounder] Sponging off others, freeloading.

COMO TIENE EL BRAZO.
COMO TRAE EL BRAZO.—(Que tira a la base certera y fuertemente).—Que está acertando, que está entrándole como el cernicero a la res.

[What an arm he has! (referring to a player who throws the bases accurately and with force)] He's an expert; he really knows what he's doing; he really does a good job. (The two Spanish expressions are equivalent.)

DE BATE EMERGENTE.—Suplenteando. Ayuda temporal.

[pinch hitter] filling in, plugging the gap.

DE PITCHER TAPON.—Idem.

[emergency relief pitcher] same as the previous entry; filling in, plugging the gap.

UNCLASSIFIED

ES CUARTO BATE EN CUALQUIER NOVENA.— Bueno a todo. Eficiente a cualquier nivel.

[he can bat fourth on any team. (Assuming that the first three men have gotten on base, the fourth man at bat—usually called "the cleanup hitter"—is expected to get a hit and score one or more of them.)] you can depend on him to do a good job; he's tops; "Old Faithful."

ES UN CARGABATES.— Un cachanachán, un hala-levas, un traca**, un perrillo faldero. En fin: una guasasa.

[he's a bat boy] he's not important, no big thing; just a lackey; low man on the totem pole. (Most of the Spanish terms used in this definition are not in standard bilingual dictionaries and are worthy of note. Unfortunately, there was an imperfection on the page at the end of the word that begins with TRACA.)

ESPERATE, QUE ESTOY AL BATE AHORA.— Llegó mi chance, mi turno, mi oportunidad.

[Wait a minute! I'm coming up to bat now] Now it's my turn; I finally got my chance! (Not quite equivalent to the English proverb "Every dog has his day," but pretty close to it.)

ESTA EN EL NOVENO INNING.—Se está acabando, falta poco para finalizar.

[We're in the ninth inning] Time is running out, not much time left; it's now or never; it's the eleventh hour.

ESTA EN 3 Y 2.—(alternativa definitoria: o le pasan un estrai y lo ponen fuera, o le pasan una bola y toma la base). —O se salva, o se hunde. Lo toma o lo deja.

[the count is 3 and 2 (it's now or never: either they'll throw him a strike and put him out or they'll give him a ball and put him on base).] The moment of truth has arrived. It's time to fish or cut bait. You have to make a decision now. (Compare ME TIENEN EN 2 ESTRAI, etc, below.)

ESTA FUERA DE JUEGO.—Perdió la puntería por falta de ejercicio, no tiene su habitual acierto.

[he's not in condition to play, out of shape] he missed the shot because he's out of practice; he's over the hill.

ESTA FUERA DEL JUEGO.—No lo llevan. Lo han desco-desconocido.

[he's not in the game] They don't even have down (on the roster); they've forgotten about him. He's a has-been.

ESTA FUERA DE SEÑA.
NO LO COGIO LA SEÑA.—No entendió, no captó lo que insinuaron. Desubicado, fuera-de-onda.

[he missed the sign; he didn't catch the sign] He didn't understand, didn't take the hint. He's not with it, in a world of his own, not tuned in to our frequency.

ESTA GUAI (wild).— La otra cara de la moneda con respecto a la expresión VIENE POR LA GOMA.

[he (the pitcher) is wild] He's not doing his job properly, he's messing things up.

ESTA JUGANDO AL DURO.—Que no afloja, que sigue los principios.

[he's playing it tight] He's not slackening up, taking shortcuts; he's following the rules, doing things according to the book.

ESTA JUGANDO AL FLOJO.—Lo contrario de la expresión anterior. Cubaneo.

[he's playing it loose] The opposite of the previous entry: He doesn't always finish what he starts.

ESTE ES OUT POR REGLA.—Sin remedio su asunto o su mal. Fracaso inevitable. Infeliz. Sin iniciativa.

[According to the rules, that's an out] There's no cure for what he has. The poor guy! He never had a chance!

ESTE ES QUIEN MANICHEA.—(de manager, director de equipo).—El que manda y también el que maneja la cosa como la de gana.

[he's the guy who manages the team] He's the one who gives the orders; he's the boss.

JUEGA TODAS LAS POSICIONES.—Superindividualista. El universal inútil hombre-orquesta.

[he plays all the positions (on the team)] Jack-of-all-trades, master of none; in a class by himself. (The Spanish uses a lovely expression: the universally useless one-man band.)

LO COGIERON FUERA DE BASE¡—Lo sorprendieron, lc pillaron, atrapado en un mal paso.

[They caught him off base.] They caught him napping, pulled the rug out from under him. They caught him (in a lie or in the act of wrongdoing).

LO DEJO CON EL BATE AL HOMBRO.—No le permitió actuar.

[He left him standing there with his bat on his shoulder] He wouldn't let the poor guy do anything; he stopped him from acting, put up roadblocks in front of him.

MANICHE DE GLORIETA.—Que critica por fuera, desde una posición cómoda, sin riesgos; pero cuando está en el agua se olvida de nadar.

[grandstand manager, manager in the bleachers] Guy who stays on the side and criticizes; a "sidewalk supervisor" or "Monday morning quarterback."

UNCLASSIFIED

UNCLASSIFIED

ME TIENEN EN 2 ESTRAI Y PELEADO CON EL AMPAYA (umpire).—Sin salvación. Agonizando.

[they've got two strikes on me and I'm quarreling with the umpire] a desperate situation; between the devil and the deep blue sea. The best I can get out of this situation is the worst.

NO LO VIO PASAR.—(la bola).—No se enteró, está como la cherna en tarima: con los ojos abiertos pero sin ver.

[he didn't even see it (the ball) go by] he wasn't paying attention; "Eyes have they but they see not" (The Spanish has a picturesque description: Like a fish in the market, with its eyes open but not seeing anything.)

NO ME PONGAS LA DE TRAPO.
NO ME PONGAS LA PODRIDA.—(En beisbol se usa pelota de "poli," que es relativamente pesada y resistente).—No me hagas la cosa imposible. No me vengas con engañifas.

[Don't throw me the ball made of rags. Don't throw the rotten (ball) at me.] Just give me the real stuff, no tricks! Don't try to cheat me!

NO SE VA CON BOLAS MALAS.—No se le puede engañar. Se lo sabe todo.

[he won't swing at bad pitches] It's not easy to pull the wool over his eyes; he wasn't born yesterday; he knows what the score is.

NO TE LANCES, QUE TE PONEN OUT.—No te atreves, que fracasas.

[Don't try to steal a base 'cause you might get put out] Don't take too many chances because you're bound to fail if you do; look before you leap; play it safe.

SE LA DEJA EN LA MANO A CUALQUIERA. —Incumplidor, falto de palabra. Dejar embarcado.

[Let somebody else catch the ball] he loves to pass the buck; he's irresponsible.

SI ME LA PASA, SE LA BATEO.—Si me alude, replico en tiempo y forma.

[If the ball comes by me, I'll bat it] If the remarks apply to me, I'll answer them duly and properly. If he provokes me, I'll get him.

TAI (time).—Tiempo, espera, tregua.

[Time!] Time out! Let's take a break!

TIENE MAS CURVAS QUE CHANGA MEDEROS.—Referido a mujer bien dotada en su diseño anatómico según el patrón criollo.

[She has more curves than Changa Mederos (a famous contemporary Cuban baseball pitcher)] Used in speaking of an especially curvaceous, well endowed woman.

VIENE POR LA GOMA (pitchea con control).—Acertado, que está planteando las cosas oportuna y certeramente.

[he throws right to the plate, he really has control when he pitches] he figures things out correctly; he always has the situation well in hand; he's very direct and accurate in his judgments, a no-nonsense type of person.

SANTIAGO "CHANGA" MEDEROS

The Spanish-language article concludes "Y... VAMOS A SUSPENDER EL JUEGO POR LLUVIA" (Let's call the game off on account of rain—an expression used to cut off a gabby person's drawn-out narration) because there are many, many more baseball terms used in everyday Cuban conversation. That also seems like a pretty appropriate way to end this English version.
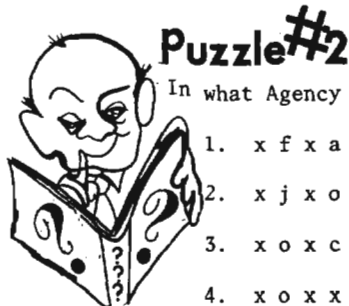
Puzzle #2

In what Agency publication would you find the following?

1. x f x a y d a s h   x j x u d i t h   x o x ' x c o n n e l l

2. x j x o h n s o n   x c x h e s t e r f i e l d   x e x

3. x o x c h s   x c x a r l   x j x ,

4. x o x x h x a r a   x d x e n n i s

5. x s x t o n e   x s s x i n c l a i r e   x m x c x k x e e

ANSWER ON PAGE 18

UNCLASSIFIED

Right-to-Left Text Sorts Are Not Impossible

by

P16
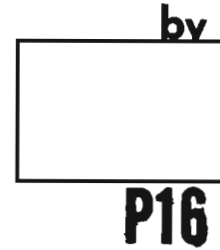
P.L. 86-36

Have you ever been faced with a pressing need for a list of data sorted in a particular way and been unable to get it? Perhaps this list of data so urgently needed contained elements of variable length such as plaintext words, and the sort sequence desired was not the "standard" left-to-right ordering of data. Does that sound familiar? I have heard of instances wherein a right-to-left word sort of data was needed--plaintext or decrypted message endings, etc.--but the computer support personnel assigned weren't sufficiently experienced in using sort routines to provide them in the form needed.

The problem at first glance seems to be that most computers only compare strings of data in a left-to-right direction. But upon closer scrutiny we see that a left-to-right comparison of the words within the data strings is what we want. The real problem is that we have to use sort routines designed for comparing fixed-length sort fields to sort variable-length data elements (words) appearing at variable positions within the data stream. For the novice programmer this may be such a formidable task that he may convince himself, and you, that it cannot be done, and leave you to waste many frustrating hours using an analytic tool that is not what you really need.

One simple solution to this problem is to generate a special fixed-length "sort key" for each data record that is to be sorted. This can be done by allocating a data field equal to a fixed maximum-word-size times the number of words wide the data is to be sorted. Sufficient textual words are then isolated, padded with blanks, and loaded in left-to-right, major-to-minor sort order into this key field. Each of these special sort keys is then either appended to the record from which it was derived or "tagged" with the location of the record from which it was derived, for use in a "tag sort" routine. After normal sorting using this special sort key, the original record is printed unaltered for the user.

As an example of how this is done, assume we have the following message endings, and the sort desired is on the last five words, with major sort on the last word and minor sort on each succeeding one to the left for up to five words:

```
001 STOP COLONEL JOHN BROWN COMMANDING
002 RETURN AT ONCE STOP BROWN
003 REPLY AT ONCE STOP BROWN
004 STOP LT. GEN. BROWN COMMANDING
```

The sort key generated would be:

COMMANDING	BROWN	JOHN	COLONEL	STOP	001
BROWN	STOP	ONCE	AT	RETURN	002
BROWN	STOP	ONCE	AT	REPLY	003
COMMANDING	BROWN	GEN.	LT.	STOP	004

The sequence listed after sorting would then be:

```
003 .....REPLY AT ONCE STOP BROWN
002 ....RETURN AT ONCE STOP BROWN
004 ....STOP LT. GEN. BROWN COMMANDING
001 STOP COLONEL JOHN BROWN COMMANDING
```

Once this basic strategy is adopted, the multitude of methods for scanning the text for word separators and moving single words into fixed-length fields to generate a sort key is limited only by the characteristics of the particular programming language being used and the ingenuity of the programmer involved. Generating this sort-key is not a trivial matter, especially using certain programming languages, but don't let anyone convince you that it is "impossible."
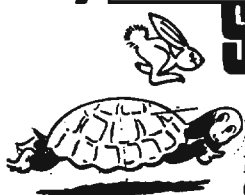
(UNCLASSIFIED)

UNCLASSIFIED

SELF-PACED INSTRUCTION: "The Future is NOW!"

by ▮▮▮▮▮▮▮▮▮▮▮▮▮▮ E13

Self-paced instruction (SPI-- sometimes called programmed instruction, self study, correspondence study, and so on) has been used at the National Cryptologic School for some time, and present planning calls for the amount of such instruction to increase greatly during the next few years. Unfortunately, few people are familiar with SPI in its new and improved form. This article presents the answers to some basic questions on the subject.

What is SPI?

SPI, as used by the National Cryptologic School, means a set of ordered instructional lessons to be mastered by the student. These lessons will combine written material with various kinds of media: tapes, slides, filmstrips, videotapes, and computer programs. Courses will be conducted in learning centers both at Fort Meade and at Friendship.

When you enroll in an SPI course you receive Lesson One which, like every other lesson in the course, starts with a list of terminal objectives telling you exactly what you are expected to learn during the lesson, the conditions under which you are to learn, and the standards you are expected to meet. In other words, you are shown the test before you start the lesson. If you wonder why we do it this way, the answer is simple: controlled studies show that students learn better knowing the objectives, as opposed to the old-fashioned method of keeping them a secret until the end of the lesson.

After reading the terminal objectives, you start to study the material. The lesson is broken down into several sections. Each section concludes with questions and exercises for you to do so that you may immediately practice what you have learned. You proceed through the lesson at your own pace. Don't worry if you get stuck at some point, a qualified instructor will be present at all times to answer any questions you may have. When you feel you have mastered the material, that is, met the terminal objectives you read at the start of the

lesson, you ask for the test on that lesson. The test checks to see whether you have indeed achieved those objectives.

If you pass the test you go on to the next lesson; if not, you go over your mistakes with the instructor and do whatever remedial work he suggests. Then when you feel you are ready, you retake the test. If you pass this time, your record shows only that you have successfully completed that lesson, and you now proceed to the next. When you have completed all the packages, you take a final test for the course, and you're done.

What is SPI not?

There are some common misconceptions about SPI. The most common is that you receive a course, are sent to a dark corner and told to remain there until you have completed it. Actually, the course will be conducted in a learning center, an area consisting of individual study areas called "carrels," where you sit while you study your text, listen to a tape, view slides, etc. The learning center is designed to be conducive to study and to make you feel comfortable. You will not be alone; other students will probably be using the learning center while you are there, and of course the instructor will be there to help you as required. You don't even have to work alone. If you are part of a small group which wishes to proceed at a common pace, that's fine. Some people learn more quickly by themselves, others prefer to be part of a group. So work alone or together--the choice is yours.

A second misconception is that you can study whatever you want. While some SPI courses offered at universities give students great latitude in choice of subject matter, ours in NCS will not. They will consist of a set of lessons which must be completed in a specified order. Therefore if you enroll in a course you must complete the specified program in order to get credit for it.

And a third is that SPI is a free ride for instructors. Certainly SPI frees me, as an instructor, from lecturing; but whereas in conventional teaching I conduct all my students

UNCLASSIFIED

through a course at the same pace, and can predict from experience many of the questions that will arise and get ready for them, in SPI each student may be at a different point in the course, and even in different courses. I'm going to have to be on my toes to handle every question that pops up.

What's in it for students?

I've already mentioned some points, but they are worth repeating. The most important is self-pacing. You're no longer locked into a fixed pace; go faster or slower, work alone or in a group, work when you want and for as long as you want, work at Fort Meade or Friendship: it's your choice. No longer will sick leave or annual leave conflict with your study. We hope eventually to have each lesson available in several different media so you can have your choice in that, too. You want to read today, but listen or watch tomorrow? SPI offers the possibility of fulfilling all choices.

Another important advantage is that you always know where you stand. In conventional courses the test usually comes too late to help. You just get a bad grade and forge ahead without any remedial work on your weaknesses. This doesn't help you, but you are kept "on schedule." With SPI and its many checks and tests--which are often self-administered--your weak areas are spotted immediately and you do remedial work to correct your deficiencies at once. Only then do you proceed to new material.

Have you ever been in a course and found some point which struck your fancy so that you wanted to follow it up? This is often impossible in conventional courses, but it is still another advantage of SPI. Follow it as far and as long as you want. Your instructor will help and encourage you. That's his job.

Have you ever been withdrawn from a course because of operational necessity? How about not being able even to enroll because the office can't spare you full-time, or even half-time? But you might have had two or three hours available each day and with SPI you could still have taken the course during those hours. Remember, you set the pace. Afraid the course will now take forever? Forget it. For most people those hour lectures become 15-20 minutes in SPI. In summary, there is just greater flexibility for you, me, and the boss.

What's in it for the instructor?

Conventional teaching forces me, the instructor, to spend many hours preparing and delivering lectures. It does not give me the opportunity to do the things studies have proved I do best: for example, diagnose your difficulties, interact with you when you need help, inspire and motivate, encourage creativity and self-direction. With SPI I have more time for these tasks. As a matter of fact, these four actions describe my job in SPI.

Another advantage is interaction with the course material. Lectures are one-way streets; I am the only active participant. Except for asking questions, you remain pretty passive. SPI forces you to interact. This is good, because studies show you learn better when you do. And if you are learning more efficiently, I'm happier.

Finally, as an instructor, I will have the time to develop the advanced and specialized courses which are needed to meet the ever-changing technology of today.

What's in it for supervisors?

Yes, there are advantages for you supervisors as well. You no longer have to give up your personnel to a rigid class schedule. You can let them take an SPI course for a few hours a day--at your convenience. Even better, you can expect them to finish the courses faster. Studies have shown that most students work more quickly with SPI than in classroom courses. A further economy is in travel time; SPI courses are to be offered at both Fort Meade and FANX. And whereas the fixed time limit of classroom teaching sometimes forces the instructor to delete material ordinarily presented, SPI courses are of standard quality and every student is given the same material.

SPI allows the Cryptologic School to help with the training of new personnel. For example a new worker in your office is unfamiliar with your type of operational problem. Perhaps Lessons X, Y, and Z of Course 000 could give him valuable background. Send him to us, we'll let him do Lessons X,Y, and Z. He won't get credit for the course, but this brief training may make him immediately valuable on the job. And don't forget that experienced workers also might benefit from a quick refresher on some aspect of a new problem.

Remember, we are not interested in training for the sake of training; we want what you want: to increase the efficiency of employees for their jobs.

What's in it for the Agency?

So far I've pointed out advantages SPI has for the student, the instructor, and the supervisor. If these advantages are real, the Agency will gain happier and more efficient employees; but more than that, it will have better trained personnel. A well-written SPI course is expected to be superior to its conventional counterpart, if only because the burden of learning is placed where it belongs: on the student. The inherent flexibility of SPI will allow more timely training for new office personnel or for that new problem which suddenly crops up.

UNCLASSIFIED

Finally, in terms of work hours lost to training, SPI courses will be much cheaper, and that is a big plus these days.

Conclusion

Does all this mean you have heard your last lecture? No, not at all. Writing SPI courses takes time and is therefore expensive. Therefore only those courses which are taught many times a year are candidates for conversion, because they become cheaper over the long run with self-pacing. I am talking, therefore, only about introductory or survey and basic courses. Advanced courses will continue to be offered conventionally. It is simply a matter of economics. However, SPI will release some instructors to develop and teach new advanced level courses which are needed.

So if you sign up for a course in the near future and find out that it's to be offered in SPI, please don't panic. As the old saying goes: Try it, you'll like it.

(UNCLASSIFIED)

A Short Directory of Career Panels

(Appointment expires)

H113 COMMUNICATIONS SECURITY

Chairman: Mr. Ryon A. Page (S4, 2365s, 8151b)   Jun 76
Executive: Mr. [   ] (H113, 2308s, 6804b)   Dec 74

H112 COMPUTER SYSTEMS

Chairman: Mr. Robert L. Hagedorn (C4, 3829s, 7980b)   May 75
Executive: Mr. Richard L. Wille (H112, 3421s, 7041b)   Oct 75

H111 CRYPTANALYSIS

Chairman: Miss [   ] (A509, 8311s, 6674b)   Jul 76
Executive: Mr. [   ] (H111, 3868s, 6629b)   Jun 75

H125 EDUCATION AND TRAINING

Chairman: Mr. Mark T. Pattie, Jr. (E3, 8041s, 6417b)   Jan 77
Executive: Mr. [   ] (E1, 8957s, 6234b)   Jan 75

H120 ENGINEERING AND PHYSICAL SCIENCE

Chairman: Mr. William H. Gossard (R13, 3031s, 7159b)   Jul 75
Executive: Mr. [   ] (H120, 4924s, 7410b)   Jun 75

H127 INDUSTRIAL PRODUCTION

Chairman: Mr. [   ] (S3, 2387s, 8133b)   Feb 77
Executive: Mr. [   ] (S321, 2191s, 6919b)   Sep 76

H114 LANGUAGE

Chairman: Dr. [   ] (P16, 3957s, 7319b)   Dec 76
Executive: Mr. [   ] (H114, 4866s, 6468b)   Dec 74

H124 LOGISTICS

Chairman: Mr. [   ] (L52, 3703s, 6757b)   Aug 75
Executive: Mr. [   ] (L11, 3281s, 7097b)   Sep 75

P.L. 86-36

UNCLASSIFIED

UNCLASSIFIED

H121	MATHEMATICS			
	Chairman:	Mr. ☐R1, 3661s, 7815b)		Apr 77
	Executive:	Mr. ☐(H121, 3957s, 7391b)		Jul 75
H122	PERSONNEL			
	Chairman:	Mr. ☐ (M3, 3393s, 7487b)		Mar 76
	Executive:	Mr. ☐(M09, 5901s, 6583b)		Jan 76
H126	RESOURCES MANAGEMENT			
	Chairman:	Mr. ☐(P, 5835s, 6521b)		Jun 76
	Executive:	Mr. ☐(H126, 3775s, 7642b)		Sep 74
H123	SECURITY			
	Chairman:	Mr. ☐(M5, 3472s, 7531b)		Jul 76
	Executive:	Mr. ☐(M55, 3602s, 6701b)		Jun 76
H116	SIGNALS ANALYSIS			
	Chairman:	Mr. ☐(W1, 5188s, 7438b)		Jun 74
	Executive:	Mr. ☐(H116, 5188s, 7438b)		Jan 75
H117	SIGNALS COLLECTION			
	Chairman:	Mr. William Hunt (K1, 3871s, 7193b)		Feb 75
	Executive:	Mr. ☐(H117, 4578s, 7911b)		Feb 77
H118	SPECIAL RESEARCH			
	Chairman:	Mr. ☐(A8, 3493s, 7397b)		Aug 76
	Executive:	Cdr. ☐(H118, 5287s, 6498b)		Feb 76
H119	TELECOMMUNICATIONS			
	Chairman:	Mr. ☐(T2, 3788s, 7044b)		Jan 77
	Executive:	Mr. Robert Poisal (H119, 4463s, 6468b)		Jun 75
H115	TRAFFIC ANALYSIS			
	Chairman:	Mr. ☐(R22, 3651s, 6429b)		Aug 75
	Executive:	Mr. ☐(H115, 4325s, 7667b)		May 77
---	TECHNICAL WRITING			
	Senior Advisor:	Mr. ☐(R4109, 4860s, 7091b)		Apr 74
---	EDITING/WRITING AND HISTORIAN			
	Senior Advisor:	Mr. ☐(E51, 8297s, 6656b)		Indef.

P.L. 86-36

(UNCLASSIFIED)

Answer to Puzzle 2: In the January 1974 Telephone Directory, on pages 26, 44, 65 and 85.

UNCLASSIFIED

NICE BUSMAN'S HOLIDAY FOR ONE NSA EMPLOYEE

BARBARA P. DUDLEY, G5

The Seventh World Congress of Translators was held in Nice from 4 to 9 May 1974, and after spending a few days in Paris (during which, among other things, I toured the Foreign Ministry, I attended the Congress as an independent observer. I estimated the total attendance as 250 to 300. The overall fee--including all the sessions, an excursion to Monte Carlo, and the gala dinner--was about $32, which I consider to be quite reasonable.

At the Congress it was interesting to compare the reports handed out by various national translators' organizations. While they all stressed the need for effective cooperation among translators to improve their lot, the American Translators' Association has been working to improve the standards of translators and translation, as well as to establish university-level accreditation programs and translator training; the French organization has been concentrating its efforts on the broadening of copyright laws to protect translators' rights; the Slovak association has been busy organizing translation activities and the criticism of translation. All stressed the need to maintain ties with other national and international associations of translators and interpreters. I have the reports from the United States, France, Great Britain, Canada, Belgium, Sweden, Yugoslavia, Czechoslovakia, and Hungary, and will gladly make copies for anyone interested in them.

I attended sessions covering the link between literary and scientific translation, translation terminology and documentation in international organizations, translation and computer techniques, and the translator's status. The papers that I found interesting were A Contrastive Analysis of Scientific and of Literary Translations by Janko Golias of Ljubljana (who stressed at the outset that he was not a member of the 60-man Yugoslav delegation), Terminology Bank and Translation by Robert Dubuc of the Terminology Bank of the University of Montreal (TERMIUM), and Data Processing at the Translator's Service by Frederick Krollman of the West German Federal Bureau of Languages.

The TERMIUM paper was of especial interest to me, and I hope that there will be an opportunity to visit the Terminology Bank "in depth" during the next Congress, which will be held in Montreal in 1977.

The most important action taken by the Congress was the recommendation of a format for the exchange of bilingual terminological information, with blocks for Semantic Unit, Source(s), and Definition(s) or Significant Context(s) in both the source and target language, plus blocks for Field(s) of Application and Author of Information Unit. /Editor's note: NSA linguists might like to compare this format with NSA Form M2424--see QRL, August 1973, page 23--or the CAMINO card./

While the formal part of the Congress was valuable and stimulating, the most interesting aspect for me was the great variety of people, a feeling which crystallized at the Gala, where the impressions came so thick and fast that I couldn't possibly recall all of them. Most of the men wore somber business suits but the women were dazzling in every kind of fancy attire and coiffure. I told the head of the European Communities' terminology committee that this was the first international gathering that I had ever attended, and that I would give anything to have it all recorded on sound-and-color film. He gallantly said, "You are an excellent observer, Madame"--I suppose that everything I was thinking about everyone could be read on my non-poker face.

My greatest thrill at the Congress came at the end of the dinner, when I summoned up courage enough to approach the eminent lexicographer Paul (le Petit and le Grand) Robert for his autograph. He is most gracious and looks as you'd expect "Monsieur Robert" to look: jovial, genial, of ruddy complexion, and apparently good for at least three more editions of his famous dictionary.

I was so impressed with the Seventh World Congress of Translators that I am already making plans to tour Quebec province in 1977 and will arrange to be in Montreal when the Eighth World Congress is in session.
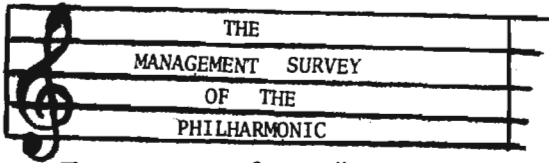
Will there be any other NSA people there?

(UNCLASSIFIED)

DEPT. OF GOLDEN OLDIES

THE MANAGEMENT SURVEY OF THE PHILHARMONIC

These excerpts from a "management survey" of the --------- Philharmonic Orchestra by the distinguished firm of Mc------ and ------ may strike a responsive chord in the souls of all those who have been, are being, or are about to be surveyed.

"...For considerable periods the four oboe players have nothing to do. Their number should be reduced and the work spread more evenly over the whole of the concert thus eliminating peaks of activity.

"All the 12 first violins were playing identical notes. This is unnecessary duplication. The staff of this section should be drastically cut. If a large volume of sound is required, it could be obtained by means of electronic amplifier apparatus.

"Much effort was absorbed in the playing of semi-quavers. This seems an excessive refinement. It is recommended that all notes be rounded up to the nearest quaver. If this were done, it would be possible to use trainees and lower grade operatives more extensively. There seems to be too much repetition of some musical passages. Scores should be drastically pruned. No useful purpose is served by repeating on the horns a passage which has already been played on the strings. It is estimated that if all redundant passages were eliminated, the whole concert time of the two hours could be reduced to 20 minutes and there would be no need for an intermission.

"The conductor agrees generally with these recommendations, but expresses the opinion that there might be some falling off in attendance. In that unlikely event it should be possible to close sections of the auditorium entirely, with a consequent saving of overhead expense, lighting, salaries for ushers, etc."

(From Hospitals, March 1954, author unknown.)

Calling all SRAs!! Reporting Symposium?

TO   : _ALL SPECIAL RESEARCH ANALYSTS_
FROM   : [   ]

SUBJECT: SYMPOSIUM ON REPORTING

I propose the holding of a two-day Symposium on Reporting as a means of supporting and encouraging continued emphasis on professional and uniform standards of reporting at the National Security Agency.

The Symposium would include major addresses by selected report editors from production elements, members of the reporting training faculty, and editors of Agency periodicals such as the _Technical Journal_ and the _Cryptologic Spectrum_. Special Research analysts would be encouraged to submit papers on trends, developments, and techniques of reporting, and the best of their efforts would be presented at the sessions. A written report of the proceedings would be published and distributed to all Special Research analysts.

If successful, the Symposium might be repeated annually.

Is there any support for this proposal? Any suggestions for the agenda? Any offers of papers or assistance?

Please address your replies to me, [   ] care of _Cryptolog_.

(UNCLASSIFIED)

Answers to Puzzle 1:

1 syllable: large charge, high spy, vile file, reel spiel, suave Slav. 2 syllables: chipper skipper, groovy movie, lighter fighter, graphic traffic, hippy crappy, marble garble, cipher lifer, sloppy copy. 3 syllables: sinister minister, quizzical physical, Egyptian conniption, astuter computer, prospective objective. 4 syllables: impudorous metropolis (!), Bavarian aquarian, ornamental Oriental. 5 syllables: tattersdemalion Pandamanian subsesquipedalion. OK, now it's your turn.

★ ★ ★ ★ ★ ★ ★ ★ ★ ★ *from the* ★ ★ ★ ★ ★ ★
PRIZES & HONORS *learned* SPRING 1974
organizations

The Crypto-Mathematics Institute awarded prizes for the following papers:

First: [   ] EO 1.4.(c)
P.L. 86-36 [   ]   P.L. 86-36

Second: [   ]

Third: [   ] " [   ] EO 1.4.(c)
P.L. 86-36

The first and third papers appeared in a Special Edition of the NSA Technical Journal
(Special Fast Fourier Transform Issue II) in August 1973. The second was published as
R111/MATH/09/74, in March 1974.

The Cryptolinguistic Association awarded prizes for the following papers:

First: "Can We Lick the Voice Problem?" [   ] Technical Journal,
Summer, 1972.

Second: "The Role of Carrier Telephony in Soviet WWII Strategic Communications,"
[   ] (to be published in the Technical Journal, Summer, 1974). P.L. 86-36

Third: [   ] [   ] QRL (Quarterly Review for
EO 1.4.(c)   Linguists), August 1973.
P.L. 86-36

The Association presented the second annual Jaffe Award for linguistic accomplishment
to Norman Wild "for his lifetime of continuing achievement and his permanent contribu-
tions in the field of language."

The Computer and Information Sciences Institute did not hold an essay contest this year,
but replaced it with a Spring Conference "to promote professional writing and to provide a
forum" for topics of current interest. Fourteen papers, chosen from those submitted, were
presented at the Conference and have now been published in the Proceedings of the CISI
Spring Conference, 21-24 May 1974. They are:

"Thoughts About System and Program Design" ....
"An Introduction to Structured Programming " ....
"Tools and Techniques in Optimization Efforts" ....
"The Insatiable Appetite of the Analyst" ....
"Large Scale File Processing--POGOL" ....
"An Interactive Display Position for the Morse Operator" ....
"A Graphics Protocol for Network Applications"...................
"The ARPANET, the COINS Network, and the Future" ....   P.L. 86-36
[   ] ....
"OMNIBUS Computer Network Communications Protocols" ....
"Minicomputers for Process Control" ....
"A Mini-Computer Speech Synthesizer" ....
"A 'Mini' Revolution in Field Processing and Reporting" ....
"A Generalized Character Input/Output System" ....
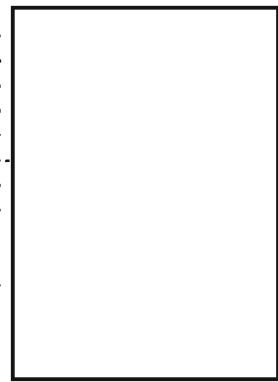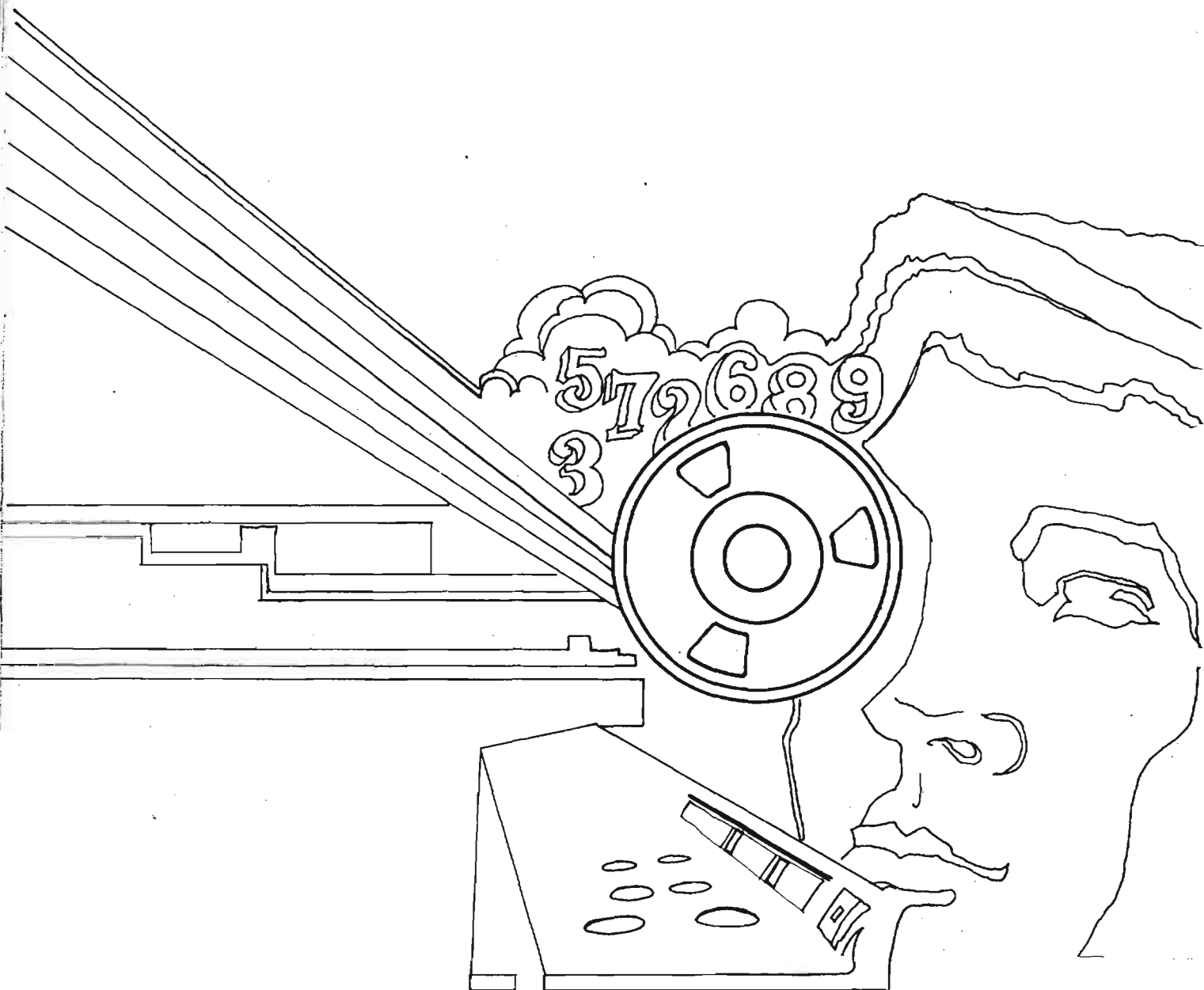
EO 1.4:(c)
P.L. 86-36   (CONFIDENTIAL HVCCO)

TOP SECRET