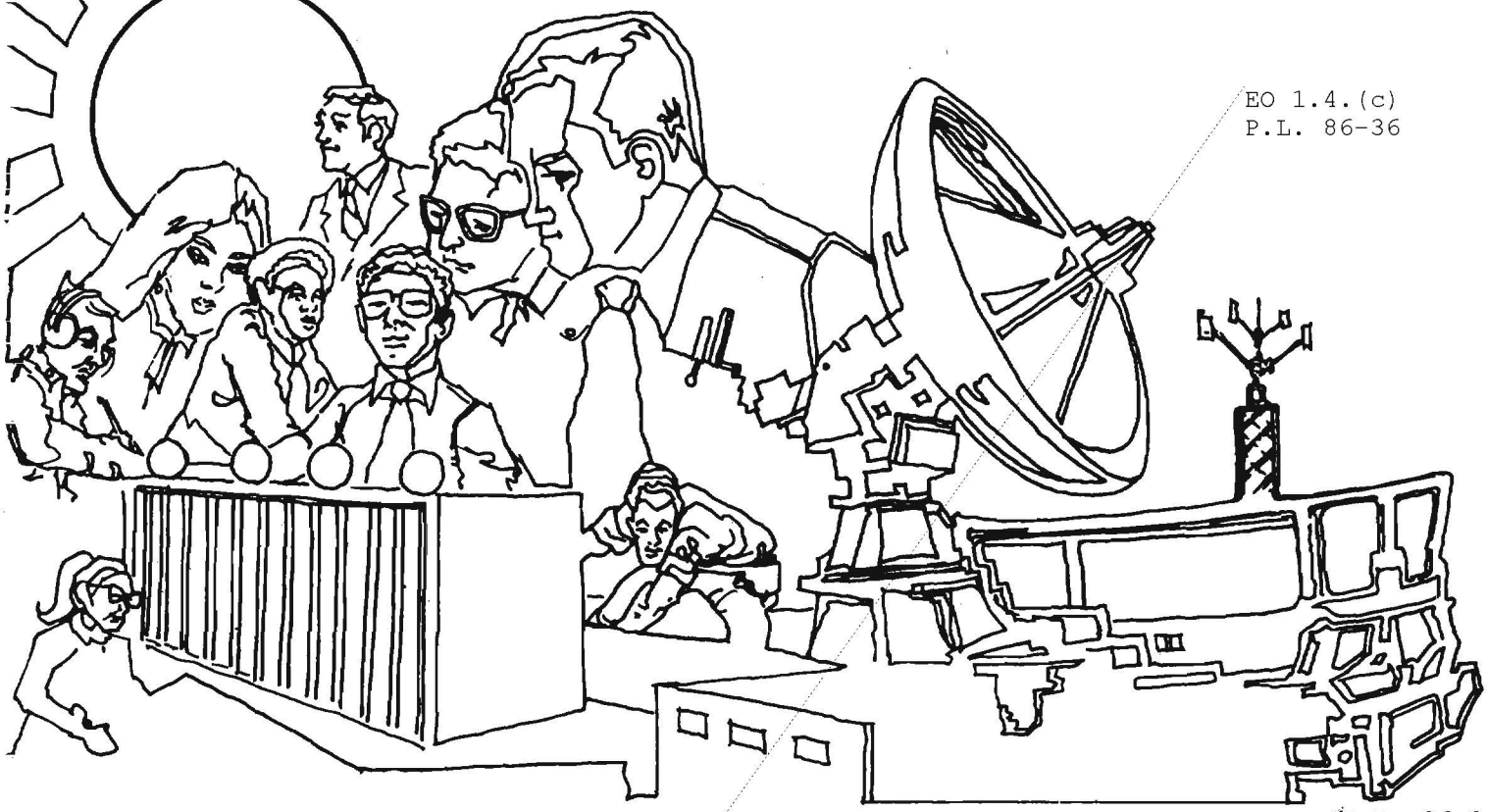
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

OCTOBER 1978



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

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. V, No. 10 OCTOBER 1978

PUBLISHER WILLIAM LUTWINIAK

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

DATA SECURITY AND HUMAN ERROR

T321

P.L. 86-36

Illustrations by the author

People are not perfect: they make mistakes. In the computer world, they make mistakes in operating machines, entering data, writing programs, and designing systems. In this article I will discuss some of the ways in which people's mistakes -- most of them caused by simple carelessness -- can cause major security violations to data in a computer-system environment.

The term "data security" refers to protection of data against persons, against modifications, or against destruction. An understanding of the number of personnel and other resources having access to information is vital to estimating exposure probability. You must also understand *how* personnel can access information. From the security point of view, a prime concern related to the data-preparation and data-control department is to protect the large quantities of data they handle from destruction and tampering of any kind.

Not only is there concern with the security of the data, but also with the validity of the data. Harm can be inflicted in several ways, such as destroying or modifying other users' data; reading or copying another user's data without knowing it; and/or degrading the service another user gets, e.g., using up all the disk space or getting more than a fair share of the processing time. An extreme case is an accident which crashes the system. This might be considered the ultimate degradation.

The security of information inside a computer system has been dealt with by several authors, who have considered the problem from a number of different points of view, ranging from privacy to government security. All those authors stress the importance of *people* in maintaining proper security. Certain people will have access to the system by virtue of their position. These include the computer operator, programmers, maintenance engineers, users, and certain management personnel. Normally these people will be able to read, modify, or copy files and programs. But all of them, being *people*, can be careless and commit serious errors. Let's look at some of them.

Keypunch Errors

Keypunch errors can cause the loss of single records and modification of records. To even the most trained eye, incorrectly punched cards look the same as punched cards containing legitimate transactions. But an error in keypunching can lead to destruction of data in a file. Keypunch errors can occur when a programmar rushes to get one last run in before the end of the day. In hurrying, he dupes a card incorrectly, throws the correct card away, and adds the incorrect card to his deck (Fig. 1).

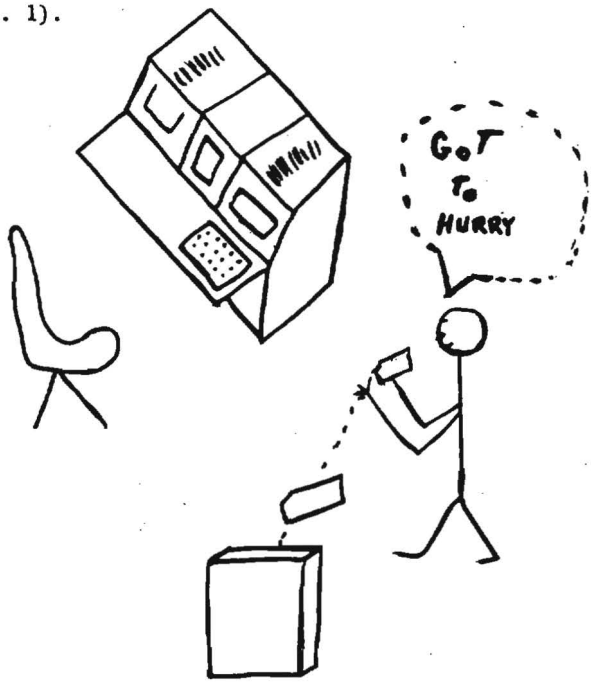


Fig. 1

Other keypunch errors occur when the computer operator is tasked to repunch cards that were destroyed by the card reader (Fig. 2).

Programmers and operators should take great care in examining the newly punched cards before entering them into the computer system.

Terminal Operator Input Errors

A user at a terminal accessing a file can cause loss of single records and modification of records.

Data preparation errors can cause a loss of data or permit erroneous data to enter the data file. When a file is initially created, the user of the file has unlimited access, to perform any of a number of operations on the file. These operations might include, for example,

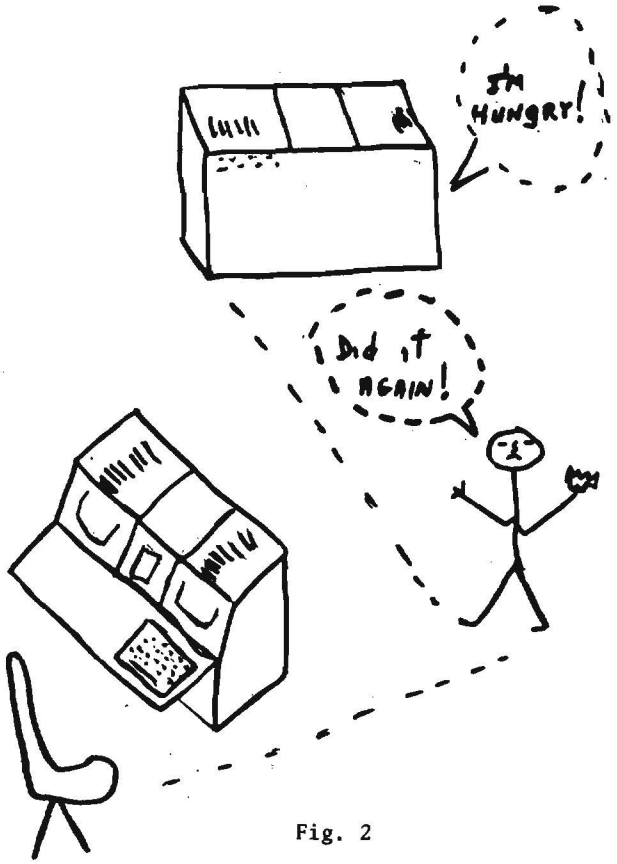


Fig. 2

reading the file, writing, emptying, renumbering, truncating (deallocating unused disk space), and renaming files (Fig. 3).

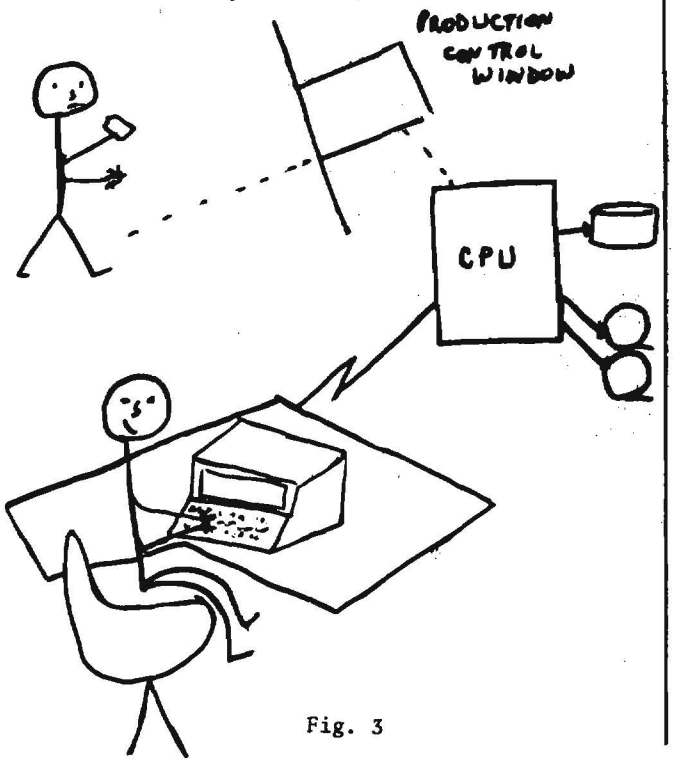


Fig. 3

Data can be destroyed in a file and replaced with inaccurate results, leaving the user with a situation where it may take considerable time to realize that he no longer has the correct data.

The user is responsible for his share of the security problem and should restrict his terminal and batch processing of files to authorized and competent personnel only.

Program Errors

Without a doubt the most common, embarrassing, and expensive software loss is program error. A not fully debugged program, coexisting with other programs, might as well be regarded as having been written by a malicious enemy -- even if all the programs have the same author. Program bugs originate because of errors in system design, errors in logic, errors in coding, errors in problem definition, or sometimes just incomplete definition. Program errors or bugs often do not show up until some *rare* combination of circumstances reveals them. They are so common that there is a regular mythology of program error (often attributed to the computer instead of the program). In some systems, a few residual bugs do not matter too much; in others they can be catastrophic.

Programs should be designed so that a user cannot alter the program. If programs are permitted to be altered, shared programs could be in a constant state of flux and this would lead to inconsistent results.

The majority of installations still have a real security gap when it comes to preventing insertion of unauthorized routines into programs.

The *Wall Street Journal* reported the Borden Company had announced a $2.8 million "deficiency resulting from what appeared to be an error in switching part of the company accounting system over to computerization two years ago" (Dennis Van Tassel, *Computer Security Management*, p. 54).

At Cape Kennedy a space launching failed because of a program error. The computer symbol equivalent of a comma was inadvertently left out of the program. The omission caused the rocket to go far off course and it had to be destroyed (*Ibid.*, p. 55).

While the impact of these two program errors is larger than most, they illustrate the possible magnitude of the problem.

The prime answer to the problems mentioned is *very* thorough program testing.

Operator Errors

Inexperienced computer operators often ignore console error messages, which can cause loss of single records, modification of records, and/or loss of an entire file (Fig. 4).

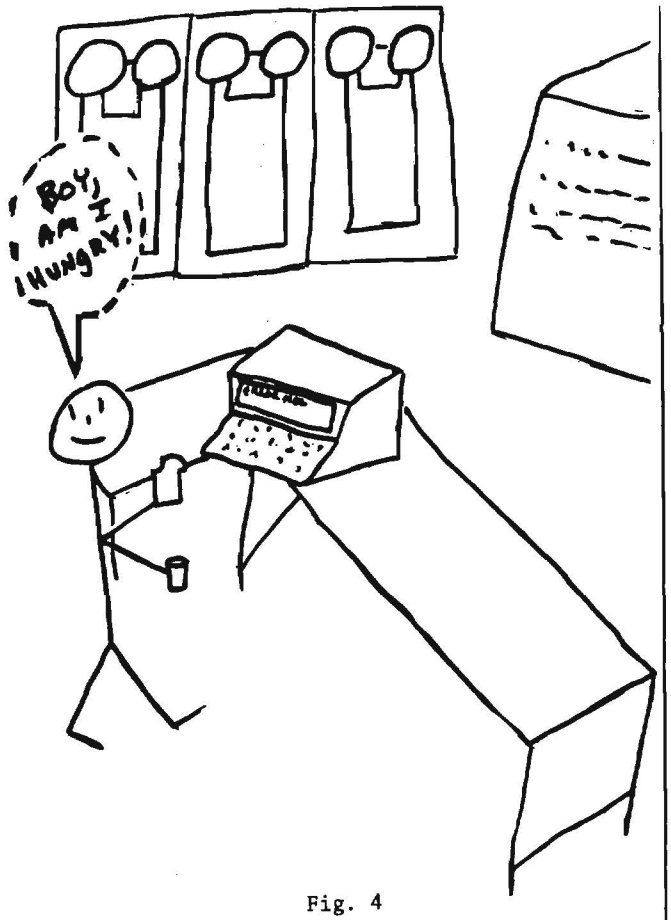


Fig. 4

The mounting of wrong tapes and/or disk packs for updating can cause a loss of entire files and modification of records. Physical damage to tapes or disk packs, such as dropping them on the floor, can cause loss of entire files or loss of single records (Fig. 5).

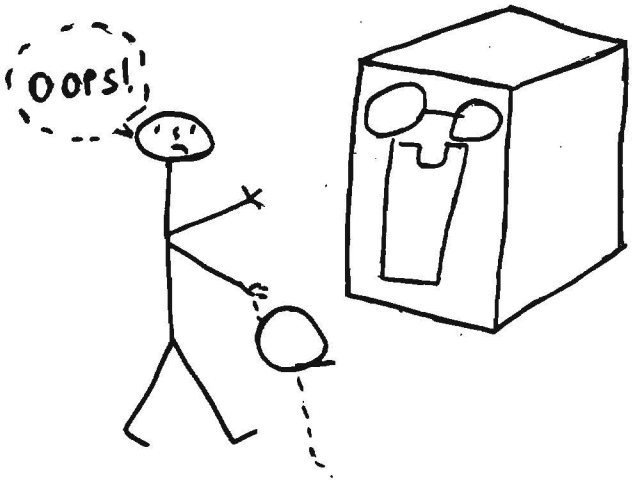


Fig. 5

Operators should be encouraged to strive for care rather than speed in handling tapes and/or disk packs.

An operator may accidentally process updates to a file twice, thus erroneously updating files. Throwing away the latest listing of an update and giving the user/programmer an earlier listing can cause the user and/or programmer to make erroneous changes to a file.

The following is an example of an operator error and what kind of problem it caused.

An operator mounted the wrong day's tapes. The program recognized the error and printed out a message saying so, but the operator ignored the message and pushed the restart button. This error was not discovered until month-end processing was completed, after which much work had to be rerun.

More care should be taken by the computer operator to assure the accuracy and safety of files kept in the computer environment.

Programmer Errors

A programmer updating the wrong version of a program can cause a loss of an entire file and/or modification of records.

A programmer who has access to the computer operations area can run his own jobs and make the same mistake an operator makes, such as mounting wrong tapes, ignoring console error messages, and/or carelessly dropping tapes or disk packs.

The following is an example of a programmer error and the damage it caused.

In August 1971 the French satellite Eole was launched by NASA as part of a cooperative French-American space program. The satellite was designed to gather data from 115 balloons, each carrying an instrument package around the earth at an altitude of 38,000 feet. On command from Eole, the balloons could transmit their information to the satellite, which in turn would relay the data to a computer center for analysis. The balloons all carried explosive charges which could detonate on a command from the satellite. On the 346th orbit of the satellite, a French programmer error caused the "Destruct" command to be sent to the satellite instead of the "Interrogate" command.

The error was discovered quickly, but before the instruction could be rescinded, the satellite had hurtled over the horizon, beyond control. A NASA spokesman said, "I couldn't tell you what happened after that; sort of chaos broke loose in the station." Eole destroyed 72 of the 115 balloons, all of those in its path on that orbit. NASA officials said the mistake resulted in some "procedural changes" at Mission Control and the possible demise of "one dumb computer programmer" (James Martin, *Security, Accuracy, and Privacy in Computer Systems*, p. 10).

Maintenance/System Errors

No system can be regarded as secure unless both the hardware and the systems programs are

designed for security.

The purpose of system controls is to prevent unacceptable data from being processed and to detect it if it does enter the system. System errors, either hardware or software, can cause a failure of one or more of the protective features. The system should be designed to log all attempts to access data files that failed due to a loss of the proper permission or password.

Conclusion

Security is only as strong as its weakest link, and the weakest link in the security chain is people. The weakness arises partly from the fact that people tend to evade or ignore the standards, and partly from the fact that people tend to concentrate on only one thing at a time. When there is pressure on the data processing department -- projects going live, last-minute modifications, emergency maintenance -- observance of standards falls off.

The value of data which is processed on computers, such as social security records and confidential information, is immeasurable. Consequently, protecting equipment and data from unauthorized or inadvertent acts of destruction, alteration, or misuse is a matter of inestimable importance.

Data processing security is a means of safeguarding hardware, software, and data against loss from accidental disclosure of data and/or modification of data.

The control of data-base vulnerability is a significant problem in many computer systems.

There is no method available for measuring the quantity or quality of security that may be adequate for a computer.

In many cases too little attention and too little money is allotted for computer security.

The effectiveness of a security system depends on the interaction of people within the data processing system. The implementation of proper procedures can help to regulate the interaction of personnel and the computer system, thus improving the security of the system.

Maintenance of security demands competence, loyalty, and integrity from all personnel connected with the system. In addition, it requires continuous training for them, both in operating procedures and in security measures. The purpose of this training is to ensure that each individual recognizes his or her vital role in security practices and does not, through familiarity with the system, become careless.

It is my opinion that each individual who is exposed to the computer environment, at periodic intervals, should familiarize himself or herself with the procedures established by management. It is up to management to see that the procedures are followed by all.

I also feel that if everyone would take more care and have more *pride* in his or her work, fewer mistakes would be made.

[redacted] *has prepared a bibliography on the topic discussed in this article. To obtain a copy, write to: CRYPTOLOG, P1, or call the editor on 5236s.* P.L. 86-36

(U)

WHO & WHOM?

By [redacted] P16 P.L. 86-36

& Nobody Else

Some people's last names have become such household words that we may forget that they have -- or had -- first names. This is especially true when two or more names get strung together. It's much easier to talk about "Lunt & Fontanne" than to throw in their first names too.

We have listed ten famous pairs on the left below and, over on the right, there are two columns of first names. In each case, the names in Column A are those of the first member in each pair, and those in Column B are those of the second member. (If we included Lunt & Fontanne "Alfred" would be in Column A and "Lynn" in Column B.)

You will note that all three columns are in alphabetical order, so, just by coincidence, a few names are in the right place. But we won't tell you how many or which ones.

	Column A	Column B
1. Barnum & Bailey	Charles	Adam W.
2. Currier & Ives	Isaac K.	Alva C.
3. Dun & Bradstreet	Merriwether	Arthur S.
4. Funk & Wagnalls	Nathaniel	Fred A. (Jr.)
5. Gilbert & Sullivan	Phineas T.	James A.
6. Lewis & Clark	Richard L.	James M.
7. Mason - Dixon	Richard W.	Jeremiah
8. Sears & Roebuck	Robert A.	John M.
9. Simon & Schuster	Robert G.	Max L.
10. Taft - Hartley	William S.	William

(Answer on page 18)

(U)

[redacted]

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

[redacted]

P.L. 86-36

[redacted]

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

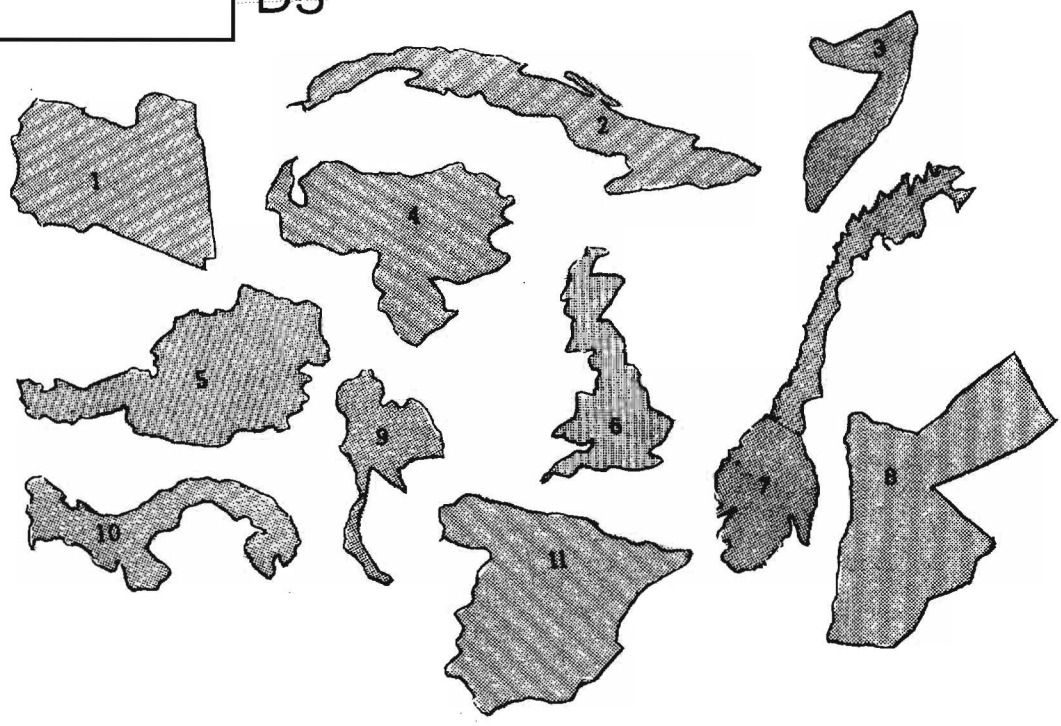
[redacted]

[redacted]

~~(TSC)~~

KNOW YOUR GEOGRAPHY

[redacted] D5



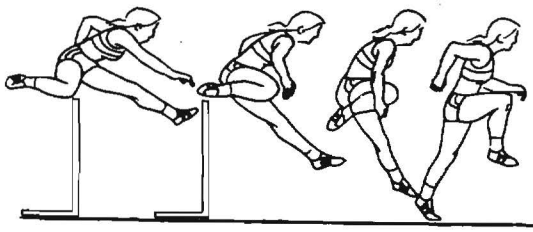
Most countries are difficult to recognize when looked at in isolation. How many of the countries shown, which are regularly in the news, can you recognize? (Countries are not drawn to scale.) If you can get more than five correct, consider yourself at the head of the class.

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____
11. _____

(Answers on page 19)

(U)

CONTINUING PROFESSIONALIZATION



P.L. 86-36

The prospect of a postprofessionalization program seems to loom in the future. A viable alternative would be to create a "continuing" system that included all people within a given career field. It would mean starting anew and rethinking the scope, purpose, and objectives of the present system. Since most of us now have a stake in the present system we might tend to deem any new system as threatening. Thus, any changes to the present professionalization program will undoubtedly be gradual and incremental with little likelihood of any radical departure from what exists now. A revolution in professionalization cannot occur, however, unless someone makes the leap to begin the struggle for change. The following is my rationale for a "continuing" system.

All current professionalization programs at NSA have varying types of requirements with assigned point values given to them. Secondly, all have a target point at which that final hurdle is completed and professionalization is yours. Following professionalization, your records are returned to you and you become a statistic. There are few pressures on you either to maintain or to improve yourself within your career field from self-motivation and a certain amount of organizational peer pressure.

It is the view of this writer that all professionalization programs should have no final hurdles. The scope of these programs should be large enough so as to include all people who choose to call themselves a professional. There should be requirements within the system to make it necessary for everyone within the field to both maintain and improve their skills. The assumption here is that there is always more to learn and time to improve, no matter how much you have distinguished yourself within a particular career field. Secondly, professionalization should serve as a measure of a person's skill and worth -- at least from a technical point of view. Professionalization should guide people toward achievement and increase their motivation throughout their career. All work would then follow the path of the high achievers, if the professionalization requirements are skillfully and fairly established and maintained.

Professionalization panels should be people-oriented and serve more as the employee "union" representative vis-a-vis organizational prerogatives. Secondly, the panels should get out of all forms of testing and leave this function in the hands of the Training School. Within guidelines, panels should determine the curriculum necessary for professionalization and then help people achieve their goals. With the functional control of their profession, the panels could then provide an organization with professional help as needed and remove them when necessary. NSA would then become task-oriented. The panels should also provide the lateral input to organizations so as to ensure equal career development opportunity.

Career panels with a larger scope and purpose could ensure functional equality within a given career field and thereby largely eliminate the promotional aspect of "being in the right place at the right time." Unfortunately, it is now possible for people within the same career field to be hurt more by their timing than by their ability. A person with half the ability, half the experience, and half the whatever-is-required, can now be promoted ahead of someone in the same career field who is twice as qualified. A more powerful panel would be better able to prevent such inequity.

A "continuing" professionalization program which included all people within a particular profession would better help managers to quantify people's strengths and weaknesses. It would also enable the Agency to measure statistically the professionalization programs and its people from year to year or whenever necessary. Presently, no one can quantify the statistical worth of each profession to say whether it is improving or declining in expertise. Comparisons should be possible, to provide more effective help in recruiting and career self-monitoring. Now the process is basically subjective in respect to the quality of people within a given career field. It is time for the Agency to become more scientific in its approach to professionalization and increase the level of functional inputs which could help to increase organizational output.

In order to remove any reader's fear of what a "continuing" professionalization process would involve, a hypothetical work sheet for evaluating aspirants is presented on the next page:

REQUIREMENTS FOR CERTIFICATION
BY PROFESSIONALIZATION PANEL "X"

John Doe
(NAME OF ASPIRANT)

	REFERENCE LEVELS OF EXPERTISE IN "RELATED" CATEGORIES, WITH NUMBER OF POINTS REQUIRED						PANEL AWARDS IN "NON-RELATED" CATEGORIES
	1 750	2 1600	3 2400	4 3300	5 4300	6 5200	
WORK EXPERIENCE	400	800	1200	1600	2000	2400	200
TRAINING	100	200	300	400	500	600	50
EDUCATION	50	150	250	400	600	750	25
PERFORMANCE	100	200	300	400	500	600	150
DOCUMENTATION	100	250	350	500	700	850	0
TOTAL POINTS ACCUMULATED BY ASPIRANT.....			2250				+ 425 = 2675

ASPIRANT CERTIFIABLE AT LEVEL 3

Professionalization awards would be given when a person has accumulated the required number of points for the particular level of expertise. For example, in the hypothetical instance above, 2400 points would be required for professionalization at level 3. (The point values given here are, of course, arbitrary; in the real-life situation, the point values would be assigned by the Panel and would perhaps be approved by an ad-hoc "Panel Comparability Board").

A person would be able to accumulate the required number of points from various reference levels of expertise in categories related to his field of specialization, and also from points awarded for categories pertaining to work experience, etc. which is not related to his field of specialization. The Panel awards for nonrelated categories should be assigned point values and be standard for all aspirants. For example, a person working in Special Research should be given more points for a college course in international relations than for a course in mathematics. The reverse would be true for a Mathematician. Education points should be fitted to the professional discipline.

The reference levels of expertise would help supervisors and aspirants to realize the areas of needed improvement. Each person's assets are different, and each person's professional advancement takes a different route. One person may be long on experience and short on education, and another person may be just the reverse. A glance at the chart would show the supervisor and aspirant that, if the person wants to develop his capabilities to the next higher level of expertise, he should try to bring up his totals in categories with low totals. Otherwise he might prove to be "top-heavy" in one category to the detriment of his overall career development.

In the sample work sheet above, the aspirant's accumulated points indicate that he is long on work experience and should probably try to bring up his total points in the area of education and documentation. A promotion board looking at this work sheet might wonder why, with all his experience, the person has not documented his labors for other people's benefit. Since a person's reference level of expertise as his career progresses should, ideally, be as close to the "vertical" as possible, this work sheet might indicate a reordering of some career priorities. The problem may rest with the individual or the organization. For example, the organization may not have allowed the person enough time to document his work. Alternatively, the person may not write well and may be hesitant to document his work. In that case, the supervisor could suggest that the person take a technical writing course before zeroing in on his documentation task.

The advantages of a "continuing" professionalization system are:

- It is intended as a method of quantifying a person's career from the beginning to to the end;
- There are no "final hurdles" which artificially handicap a person;
- A person could be better identified according to his expertise in different career fields. For example, a person might be a level-1 Collection Operations Officer, a level-2 Special Research Analyst, and a level-3 Traffic Analyst;
- The system would provide for complete quantification of skill levels within a career field. This would aid management by increasing the efficiency in recruiting, staffing, transferring, and promoting people; and
- People would be more motivated to improve their professional skills.

The greatest disadvantage of the proposed scheme is that it makes the present professionalization system obsolete. This would be the largest of all hurdles to overcome. To this writer, however, the concept of "continuing" professionalization is vastly superior to any program of postprofessionalization.

A METHOD OF MEASURING [redacted] INTELLIGENCE

[redacted] ex-W322

When the author of this article submitted it to CRYPTOLOG in April, he stated that he had deliberately omitted much of the more technical detail, such as how the probability figures are derived, but offered to answer any questions that the published article might engender. Unfortunately, that offer no longer applies, since the author resigned in late June 1978. Questions may, however, be directed to his former associates in W322, on 3764s.

[redacted]
Collection Editor

[redacted] article in the April 1978 CRYPTOLOG ("We Gotta Accentuate the Negative") pointed out the problems that exist with intelligence efforts that yield negative results. The challenge is to make the most of such results and produce negative, but useful, intelligence. This article will attempt to describe a method developed by [redacted]

[redacted]

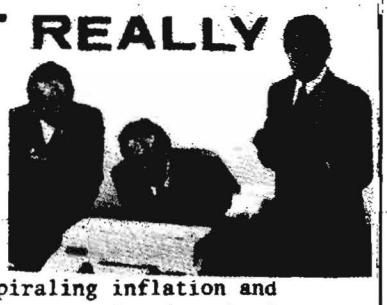
[redacted]

[redacted]

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

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

WILL IT REALLY DO THE JOB?



T2141

In a day of spiraling inflation and spiraling computer-related technology, the staid method of selecting the best equipment may be impractical. If we select an equipment only for its ability to perform, we will more than likely ignore several other crucial criteria. If criteria such as those I have in mind are ignored, our future operations may be seriously hampered.

It was once said that he who has not learned from his past mistakes is condemned to relive them. And relive them he will, unless flexibility of technology is one prime consideration in selecting an equipment. What degree of flexibility is built into the technology of a contemplated purchase? The knowledge of built-in flexibility would certainly be a comforting thought when -- and it is is inevitable -- the accelerating spiral of technology catches up. At this time one must either put the equipment to new visionary use or plan for a new purchase.

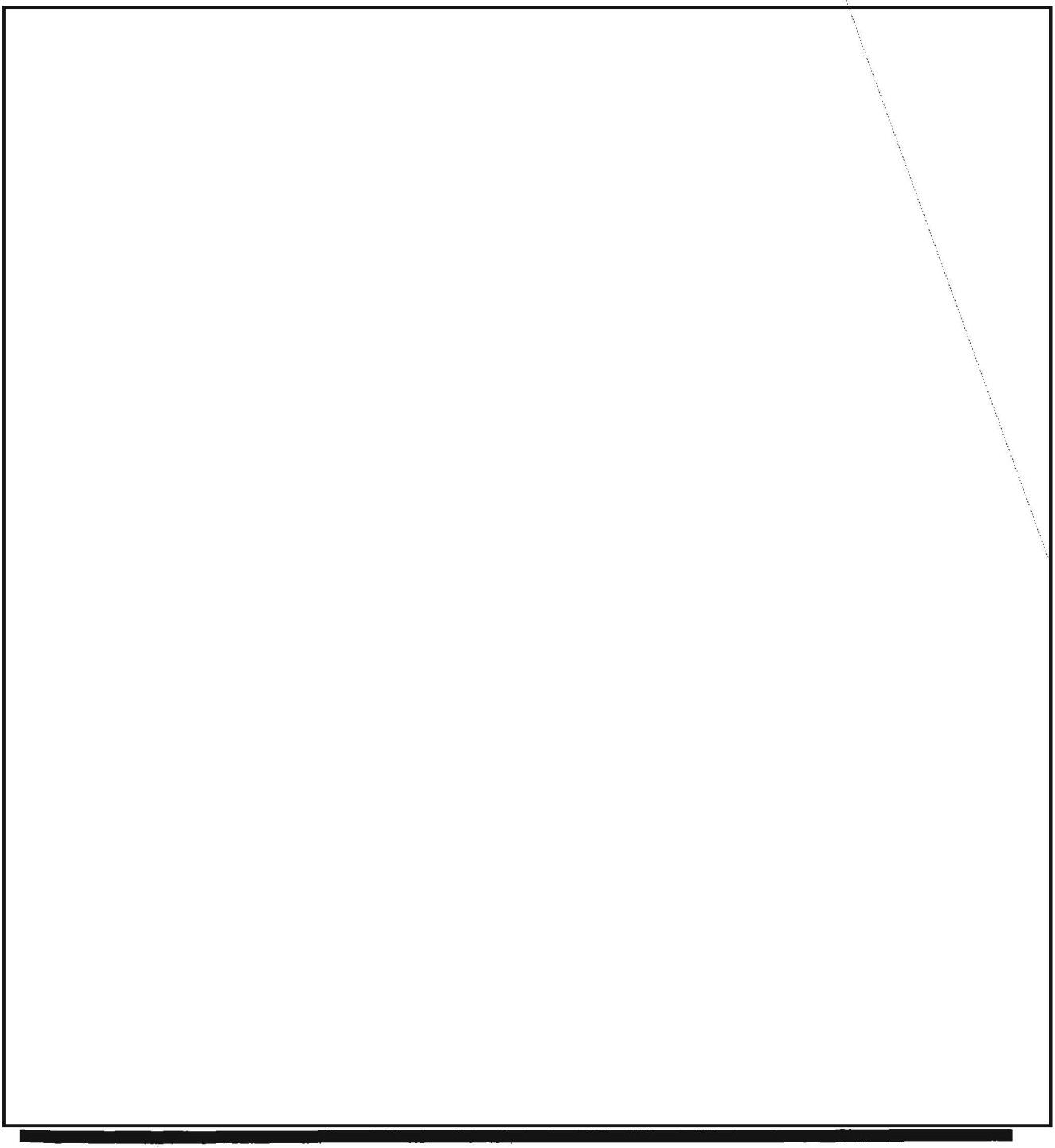
On the other hand, what we buy we must support. Several questions should surface in this area. These questions center around the contractor's ability and willingness to furnish a constant stream of technical support for an equipment he wants to sell. So we ask, does the contractor have a maintenance team available? Can we easily identify and obtain replacement parts? Are good technical manuals available, including logic drawings and technical changes? Does the contractor give training courses on his equipment? Does he have both the ability and the willingness to develop software and drawings specifically for our needs? P.L. 86-36

It is this type of thinking that conveys to the contractor the message that the equipment he sells in June, he must support in December.

It is needless to say that all these considerations are necessary during the preliminary planning stages. Otherwise we may abruptly discover that the ideal equipment may fall far short for extended use and be doomed to a very short life cycle. (U)

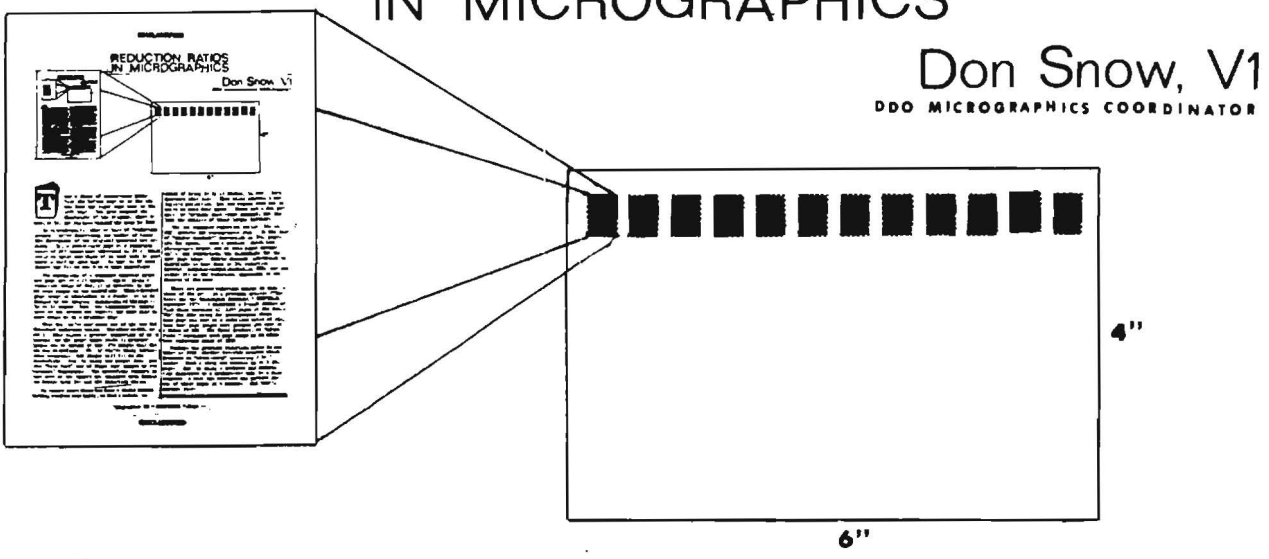
YOU CAN'T TELL THE WHEAT FROM THE CHAFF WITHOUT A PROGRAM

J. Gurin, R5



REDUCTION RATIOS IN MICROGRAPHICS

Don Snow, V1
DDO MICROGRAPHICS COORDINATOR



Take a sheet of letter-size paper. Fold the bottom edge up to the top. Now fold the right edge over to the left edge. You have reduced the *dimensions* of the original sheet by two, or 2X; but you have reduced the *area* by four.

In micrographics, when we talk of "reduction ratios," we're describing the number of times the *dimensions* of the original material are reduced. So, a letter-size page at a reduction ratio of 24X (sometimes expressed as 24:1) would yield an image one-third of an inch wide by just under a half an inch high. As many as 98 such images can fit on one 4-by-6 inch microfiche.

The dimensions of a standard computer printout page are 14 x 11 inches. Again, using a reduction ratio of 24X, it is possible to put 63 such images on one microfiche. When a desired page image is positioned in a reader, it is enlarged to the original dimensions of the page -- 14 by 11 inches; thus, the alphanumeric characters on the screen are exactly the same size as they would be on a printout page.

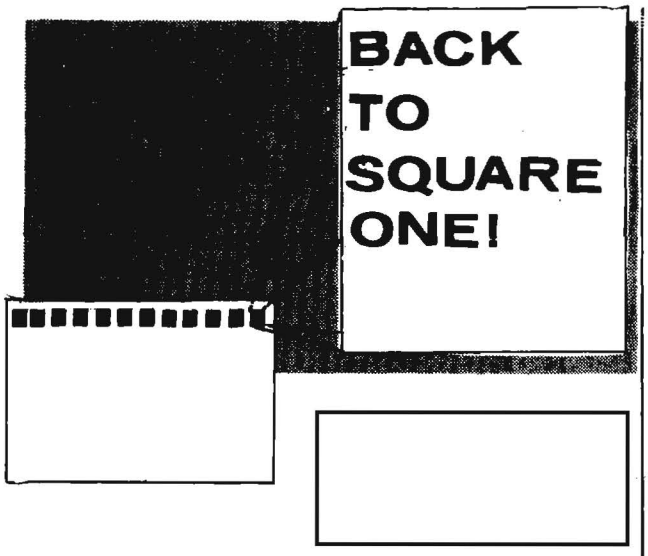
Thus far, we've mentioned one of the two DoD standard reduction ratios. The other is 48X, or 48:1. This allows a greater compaction of material, to the point where 14-by-11 printout pages can be shrunk so that 270 images will fit on one microfiche. Or, if you're using letter-size originals, 420 images will fit on one microfiche. And, by using the proper lens, you can "blow back" one of those tiny images to its original dimensions. The microfiche readers in use here at the Agency are equipped with lenses to handle both 24X and 48X reduction ratios.

In recent years there has been a trend toward making readers less bulky, so that a screen, instead of being 14 by 11 inches, is about three-quarters that size. That still affords a very legible projection, but the reader does not require as much desk space. There are a few portable, or "attaché case"-type readers, but they lack the quality of their larger brothers.

The two standard reduction ratios, 24X and 48X, involve one photographic step. In the case of "source document" conversion at 24X, pages are fed manually into a machine, which then photographs either one or both sides automatically, and repositions the microfiche for the next page image. Source document conversion to microfiche is best done at 24X reduction; however, computer-output-microfilm (COM) may use either 24X or 48X reduction, depending on the desires of the user.

There are greater reduction ratios in today's state of the art. In a previous article ("The Bible and the Washington Monument," CRYPTOLOG, September 1976), I described a 2-inch square of film which contains all 1245 pages of the Bible. That was done using *two* photographic steps: each page was shot at a reduction ratio of 15X; then four page images were grouped and shot at a ratio of 10X. The final product, or "ultrafiche," contained each page image at an effective reduction ratio of 150X.

Perhaps the greatest reduction ratio in use today is 210X, another two-step process which produces an "ultra-strip" measuring 1 by 7 inches. Such a strip can contain up to 2,000 pages! And, by using a keyboard and information displayed on a cathode-ray tube by a minicomputer, a user can retrieve and project any one of those pages in 4 seconds. But that's another story!



The trend toward microforms in all categories of publications seems to be facing a setback. The publishers of the *American Journal of Computational Linguistics*, which has been sponsored since 1974 by the Association for Computational Linguistics in a 20X microfiche format, have recently polled the membership about format preferences. Although previous membership samples have indicated support for the compact format, this latest request for direction from the membership is couched as an appeal for a change to a more traditional format such as used by the *Communications of the ACM* and the various *IEEE Transactions*. The reason? To increase the readership and consequently the rate of submission of technical articles. Production costs would approximate those currently sustained, and it would even be possible to produce the microfiche too for very little more.

P.L. 86-36

Whatever the eventual outcome for *AJCL*, the apparent low readership seems to be attributable to the alien format. Much as I have supported the use of microforms for active files and other uses, I must confess my own response to *AJCL* microfiches has been lukewarm. Although I like being able to keep a complete set of copies in a 4x6" card file, I just can't curl up in an easy chair with a microfiche reader for an evening of professional enlightenment. Is there a solution that the human factors engineers have missed?

(U)

OVERHEARD WHILE STANDING IN THE BURN-BAG LINE

On two days in a row [redacted] submitted to the editor a quote that had been "overheard while standing in the burn-bag line." If that isn't enough reason for initiating a new CRYPTOLOG department, I don't know what is!

The quotes are:

"If they *really* want that many linguists around here, why doesn't the Director hold his staff meetings in Russian?"

"Working all day long on that scope isn't as bad as I thought. I keep a book nearby and whenever the system goes down, there isn't anything to do, so I read. It's all very uplifting. I'm going to read *War and Peace*. The guy beside me is studying law. . ."

Have you overheard anything interesting while standing in the burn-bag line? If so, send it along to this department. Sign your name or keep it anonymous -- it's up to you.

(Hint to would-be authors: Keeping an ear open while you're standing in the line yourself, or keeping an eye open while reading this department might give you an idea for a CRYPTOLOG article -- such as "Is Down-Time Excessive?")

P.L. 86-36

(U)

FEEDING THE GERMANS MISINFORMATION

P. W. FILBY

Review of: *Beyond Top Secret Ultra*, by Ewen Montagu. Coward, McCann & Geoghegan, 192 pp., $7.95.

Sir John Masterman in his *The Double Cross System in the War of 1939 to 1945*, published in 1972, told how German spies were captured and then used to feed false information to the Germans. At that time the existence of the cipher systems classified Ultra, which were broken by the British at Bletchley, were still under wraps, and Sir John had to use only information which came from other sources. Now Ewen Montagu, a distinguished judge, has produced the complement to Sir John's book in his recollection of double-cross and the manner in which, through Ultra, success or failure could be judged. Some who worked at Bletchley deplore the publication of Winterbotham's *The Ultra Secret**, but readers will be enchanted by Ewen Montagu's book because he is able to use all the secret intelligence gained through Ultra.

Many readers will remember the startling story written by Montagu called *The Man Who Never Was*, about floating a body bearing war plans into Spain (Operation Mincemeat). At the time Montagu could not tell his public that the fact that the Germans bit the whole deception was ascertained from Ultra messages. Now he treats his readers to a tour-de-force on the way the Germans were fed with much misinformation through German spies who were "turned round." He names agents and tells how, when caught, they accepted the role of double agent and played supremely well and fairly on the Allies' behalf. Moreover, through Ultra the British could check on the manner in which the Germans accepted the information and whether an agent had been "blown." Montagu recounts several astonishing and exciting stories of narrow escapes and surprisingly records that in spite of the steps needed to get false information to the Germans the stories were accepted without much question, and one or two star agents were awarded the Iron Cross! Perhaps the most astonishing statement is that throughout the war every agent was caught within a few days of arrival, probably because of England's being a "tight little island."

Ewen Montagu had been called to the bar in 1924. When war broke out he joined the Navy and was assigned to low-level intelligence, but such was his brilliance that he soon became one of the handlers of much of the highest-level intelligence of the war. He tells without bitterness how his meteoric rise was not matched with corresponding promotion, and he remained a Lieutenant Commander for the whole of the war. (Being missed out for promotion was the fate of many cryptanalysts also!) With his wife in the United States he was still forbidden to stay one day over the week demanded by his discussions with his American opposite numbers in Washington.

Readers might also like to picture security in those days. Montagu had to travel between departments with top secret papers and he reports that this put him in a dilemma. He writes, "This problem I solved by fixing a large metal basket-type carrier to the front of the cycle. To this I chained the brief-case when it was parked. There was some doubt about the security of the operation for such 'hot' documents, but I managed to get permission to adopt it as long as I always wore a shoulder-holster and automatic pistol."

Montagu became one of the very few to be let in on Ultra; he attended the famous XX Committee, which met weekly to decide on deceptions to be tried, and therefore needed the information. He had two roles: supplier of information to the Services and producer of "chicken feed" or misinformation to the enemy. He tells story after story, all with undoubted authenticity. Because of Operation Mincemeat Hitler kept forces in the wrong place for over a year while Italy was being invaded, still believing that the main thrust would be on the west coast of Greece and Sardinia. When the invasion of Normandy was imminent the Germans had to defend the Pas de Calais long after the Allies had a firm hold in France, simply because Montagu's team had reported a great build-up in the Dover area. He had trouble when there was a moral issue. Should he report to the Germans that the U-boat commanders, the German Navy's heroes, were traitors? No. But when flying bombs fell in London, should he get the Germans to believe they were overshooting? Yes, because fewer lives would be lost to bombs falling short of densely populated London.

One might wonder how the Germans were tricked so often. Well, not all the information was wrong. Quite often the Allies released perfectly valid information -- just a little too late for any great value to be gained, but the Germans could prove the information correct and the agent therefore reliable.

In this book Ewen Montagu has produced the most exciting of all the Ultra revelations to appear so far.

During World War II the author was an officer in Military Intelligence at Bletchley.

*See CRYPTOLOG, December 1975: "Winterbotham's 'The Ultra Secret' -- Three Views": "A Personal Comment," by Brigadier John H. Tiltman; "Ultra Was Secret Weapon That Helped Defeat Nazis," by P. W. Filby; and "Mum's *Still* the Word!", by Paul R. Hutchinson.

[redacted] said,

P.L. 86-36

[redacted] adds,

...AND-A YOU BETTA HAVE MOTI-VAYSH!

O.K., CRYPTOLOG, you finally got my attention! At the risk of falling for a belated cryptologic April Fool's gag, I really have to comment on [redacted] article "Uncle-a Sam Wantsa You!" (CRYPTOLOG, May 1978).

At the end of his article [redacted] offers the opinion that, when recruiting linguists, high ambition in the applicant should be viewed as a criterion for *non*selection. He goes on to state that the problem with highly motivated people is that they expect (and emotionally require) high productivity to be rewarded, and government service is not set up to give rewards for productivity. [redacted] then offers us a formula for recruiting linguists: "If the object is to recruit career linguists, no more than a moderate amount of ambition or motivation should be allowed in a recruit."

Assuming [redacted] is really serious (and I applaud his motivation in undertaking this ambitious article) I strongly differ with his viewpoint. From time to time in the past we've been through this "hire the poor and keep 'em without shoes" syndrome at NSA. The problem is that people's aspirations change as they mature and after they have satisfied their basic needs (get a job and eat regularly). Inevitably some percent of the supposedly unmotivated work force begins to show "dangerous" inclinations toward greater responsibility, take new and nonstandard approaches to their jobs, and (horrors!) begin sinfully lusting after positions where they can influence how and why things are done, rather than to gratefully accept their designated place in the "system." When you think about it, Thomas Edison turned out to have been a pretty poor selection when he was hired as a newsboy. True, he eventually revolutionized communications rather than just delivering them, but you can bet that the guys down at the newspaper's recruiting department didn't see it that way, and redoubled their efforts to find a replacement who would be satisfied with just delivering the damn newspapers.

Let's face it, our future key people will not have been hired in response to a want-ad for "Key People Wanted," but will come from among us, perhaps even to include a maverick linguist or two (to the eternal anguish of those who recruited them as linguists). With a little luck they'll have the moxie to solve the "linguist problem" that has eluded the rest of us for so long.

I also question the validity of [redacted] contention that" government service is not set up to give rewards for productivity." In my view that depends on one's perception of "rewards," and in addition to the bucks involved in rewarding people (important), there are other intangibles which weigh heavily in job satisfaction and the resulting work force stability.

Since I'm apparently the only person in the cryptologic community not previously embroiled in the "linguist issue," here's my two cents' worth:

- Hire the most motivated, most ambitious linguists you can find.
- Tell them *up front* about the problems of day-to-day language work and the riptide of opinion that prevails on how to acquire and keep a linguistic work force.
- Challenge them to solve our problems.
- Listen to what they say after they have some experience.
- Enrich their jobs, encouraging them to stay in the field. Pay them fairly.
- Disregard all they say upon entry about being satisfied doing the exact job they're hired to do.

My theory is that, at recruitment interviews, people tend to tell us what they think we want to hear.

Interviewer: "And do you think you'll like the work?"

Applicant: "Actually, ever since I was a small child I've had an insatiable desire to sit at a desk and translate all day. When all my friends were out playing, I used to translate the labels off of olive-oil cans."

Virtually all will profess a love of doing the job we have in mind for them, vowing no

aspirations for other things. Once hired, however, a bunch of them will begin their private guerrilla campaign for the Directorate, and, for them, their entry job is only a first step. Great!

To hire unambitious workers as a matter of policy, as [redacted] suggests, is to give validity to the claim that we have in fact become a true old-line bureaucracy and are proud of it.

Our goal has got to be to make our linguists' work more interesting, rewarding, and challenging, and to make an NSA linguistic career a desirable profession rather than a feudal system where the linguist vassals gratefully accept their piecework assignments.

From the symptoms evident to me (a non-linguist), it seems that we have not managed our language people (among others) and their tasks in a way that works both for linguists and management. The danger is that we will default to a mode of the self-fulfilling prophecy, where we hire unambitious people who will then indeed rise to the challenge and become and remain truly mediocre.

P.L. 86-36

P.S. Since writing the above, I have had second thoughts about a work force composed of unmotivated, unambitious people. I have been able to locate several linguists who seem to meet [redacted] standards for low motivation and lack of ambition and would make ideal experimental subjects to test his thesis. Unfortunately, I have been unable to get them to take the initiative and get their applications in for consideration. (U)

News of the Communications Analysis Association

By W.E.S.

If you have ever recovered a frequency rota, or broken an authenticator system, or figured out how an address table works, then you have been *doing* Crypto-TA, whether you realized it or not.

Most analysts need to understand enough about this subject so they can (1) solve their own simple problems as they come across them, and (2) recognize when they need "specialist" help. And there are a few people around who have the interest and ability to get deeper into the "specialist" aspects of the subject. If either of these descriptions seems to fit you, then you ought to get in touch with the CTASIG (Crypto-TA Special Interest Group) and find out what they can do for you. Among the people you might contact are: [redacted], and Fred Mason.

~~(C)~~

A follow-up discussion on the subject "Interstellar SIGINT" was conducted on 14 August 1978 for some 20 CAA members. [redacted] Chief, W16, gave a short recap of the presentation he had given in the NSA Auditorium on 28 June 1978 and then entertained questions. The session lasted about one hour -- members present came prepared with very interesting questions. A transcript of the 28 June talk is now being edited for publication in a future issue of CRYPTOLOG. (U)

Meet our Program Chairman!

[redacted] has been in the cryptologic business since 1947. After 5 years with the Naval Security element in Washington, D. C. as a Communications Technician, he converted to civilian status in February 1952 and went to work at Arlington Hall Station. Hired as a Communications Clerk, he performed traffic analysis on [redacted] (printer and Morse) and served as a section reporter through November 1956. He joined the Office of Training as a TA Instructor for a two-year tour and stayed 13 years. After teaching Basic Radio Communications and Traffic Analysis for some 4 years, he then developed and taught Traffic Analysis, Technical Reporting, and SIGINT Reporting courses. He served as the Training advisor to the TA Career Panel when it was first formed and was selected to serve as the NSA Pacific Staff Training Representative. Prior to his departure for the overseas assignment in the summer of 1967, he served as the Executive for an ad-hoc group charged with determining whether or not Education and Training should be considered a career field with criteria for professionalization established. Earl was instrumental in establishing that set of criteria before leaving for the NSAPAC job. After 2 years in Japan with many trips throughout the Far East, he returned to the NCS (National Cryptologic School) Staff at Fort Meade and was assigned to investigate the possibility of setting up a training course for troopers on their way to Korea, similar to the TA operational training given to troops on their way to Vietnam.

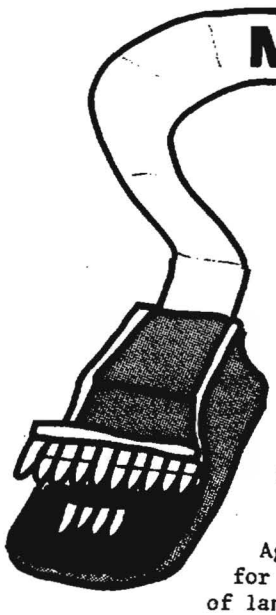
He then assumed the responsiblity as Chief of the TA Training Department of NCS for approximately one year before accepting the appointment as Executive to the TA Career Panel in May 1970. His term expired in May 1973 but was extended for one year. In May 1974 he transferred to R221, "HF Systems Architecture" Project Management. In July 1976 he was appointed TA Executive again and currently serves in that capacity. ~~(S - CCO)~~

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

P.L. 86-36

MORE B.S. (Before SPELLMAN)

[redacted] G03



Another "remembrance of projects past," prompted by Jack Gurin's "Never Again!" (CRYPTOLOG, June 1978) and A. Salemme's follow-up to it, "I Remember SPELLMAN" (CRYPTOLOG, July-August 1978).

Once upon a time (1956) a tender soul (me) was employed by the Agency, which was looking for someone with knowledge of languages, area studies, and intelligence background other than COMINT. And so I became a minion in the TNG (Training) fiefdom of the late lamented Shelby P., where books on desks had to be aligned by size (and not by content) from left to right, where suit coats had to be worn anytime you left your desk for a trip to the you-know-what, and where everything, including thoughts, was hierarchically structured.

But times were changing and even Camelot looked outwards. And one day someone decided that the Agency should look into "management theory." So, soon TNG hired a couple of fellows who would dream up management courses. Their room was next to mine, in fact their entrance was through my office, so I overheard many of the surmisings that eventually found their way into the first trial and proto-seminars -- we, next door, laughed at the absurdity of most of their notions, but of course such endeavors have long since been anointed as the Holy Grail and are believed in by people who look askance at ESP, flying saucers, and all of Serendip. About that time the concept of "brainstorming" was trying out its wings in the world, and of course the management people picked up on that gimmick.

Thus is came to pass in the TNG fiefdom that the Grand Vizier (about that same time Lambros Callimahos took upon himself the title of Guru) promulgated an edict to the effect that on Friday mornings assembled his minions would brainstorm in his presence. His minion of the Irish persuasion soon asked for support from his own subminions, so, mightily did [redacted] myself, and others come up with seed ideas and other things for brainstorming input.

One of these ideas for the brainstorming sessions had to do with -- would you believe? -- stenotypy and possible ways of having transcription done by people with less than the five years' experience with spoken Russian that is required to do professional-level transcription. Whether that idea was ever thrown into the Friday brainstorming hopper or not, I do not know. But herewith is the exegesis of that particular ploy.

In 1949-1950 I had been an English-language teacher at the Lycée Henri IV in Paris. One of my students there was also studying stenotypy at the Grandjean (?Grand Jean) Institute, or was it the Grandjean system? I don't recall. Anyway, that student and a couple of other stenotypy students asked me to help them -- they needed American speech they could practice their stenotypy on. I obliged. One of the students was French-born but the child of Polish refugees. She knew French, Polish, some German, and was perfecting her English. Students of the Grandjean system in Paris were of very diverse backgrounds, coming from all over Europe and from the various French colonies. Therefore, by design, the Grandjean system as taught there was deeply influenced by phonological theory. My little Polish student found it easy to use her stenotype machine to record Polish and English as well as French.

But back to Camelot! During my early years with NSA I lived at Hartnett Hall, where we had a TV room. At 6 p.m. every night two of the Hartnett Hall residents, one of whom was taking stenotypy at some local school, would take their seats, stenotype machines in hand, and practice transcribing the news broadcasts. One night there was possibly up to a minute's worth of foreign language on the news (probably De Gaulle), and I noted that one of the stenotypists continued to stenotype without a break. After the news broadcast was over, I remarked to him that I didn't know that he knew French and his reply was that he didn't -- he was just practicing the sounds he heard. He ran through his roll of tape until he found the proper spot and then pronounced what he had on paper. I could understand it, but he couldn't. It was sort of like the old gimmick of asking a French speaker to read aloud the nonsense phrase "pas de leur Rhône que nous!" in front

of nonspeakers of French, and have the latter burst forth in laughter while the French speaker is totally nonplussed, since the phrase makes no sense -- after all, he is filtering the words and sounds through the French phonemic pattern and doesn't realize that his audience is filtering the sounds through the English phonemic pattern and is hearing "Paddle your own canoe!" Q.E.D., I had learned that it is possible for a person to transcribe a little bit of a foreign language he doesn't even know (Note: This was a highly trained stenotypist who was already working for the D. C. court system).

As a person with a degree in Chinese from Harvard and a Master's in French from Middlebury, plus experience as an announcer in Spanish and Portuguese on WLW short wave in Cincinnati, and an immediate background as an interrogator in German for the USAREUR Intelligence Center, I should have known that my first major assignment at the Agency would be the teaching of Polish. That meant that we hired the Georgetown University Polish instructor as a contract employee of the Sanz School of Languages to get my feet wet and bring me up to speed to take courses from him at Georgetown. The environment at the Georgetown School of Languages and Linguistics, plus the heady atmosphere of the PATA (Promotion and Training Agreement) Program in TNG, in which the students were introduced to the concepts of linguistics (using the Gleason textbook), soon got me into formal linguistics.

And thus the stage was set. Then came brainstorming.

The concept as I came up with it was as follows. Some high-school students would take typing and steno*graphy*. It should be possible to select some people from that population who have an aptitude for language and teach them steno*typy* and drill them in the sounds of phonology (as taught in beginning college courses in Phonetics and Phonemics, using the texts of the Summer Institute of Linguistics or other such materials). Afterwards they would be taught the sounds of Russian.

The second step would be to take a number of open-minded Russian linguists and teach *them* stenotypy. The purpose was not to turn the Russian linguists into stenotypists, but to enable them to read the stenotype tapes made by the non-Russian-speaking clerical specialists. Back in 1956 we had a Russian-language manpower shortage (we still have one, except that now it probably ought to be called a "personpower shortage") -- remember that it takes a degree in Russian and then up to 5 years' experience to become a truly professional transcriber -- but the stenotypy concept could possibly train people in 6 months or so to put onto stenotype tape information which a skilled linguist could scan for relevance and importance. Then the decision could be made to turn the tape over to a transcriber. In other words, my concept was that this was a method of making it possible to scan a far larger volume of material by eye than can be done on a 1 : 1 basis by ear.

The key and salient points of this two-step concept were:

- the careful selection of highly motivated *clerical people* and the training of them first in stenotypy and general phonology, and then specifically in the phonology of Russian; and
- the providing of hand-in-hand training in stenotypy to some *senior Russian linguists* for scanning purposes.

Never did I say that G.I.'s selected in the military manner to learn Russian at a 6-month course in Monterey should simultaneously be taught stenotypy and become stenotypy transcribers; nor that a Cyrillic keyboard would be needed; nor that this could be an input into machine translation. So you can imagine my surprise one day in 1960 when I learned what was being asked of [redacted] I stated to her then and there that it sounded like my original concept of a few years earlier, but one which had been brainstormed and confounded until there was no possible way it could succeed.

If "they" do want to try again with the stenotypy concept some day, I'd like to implore "them" to please-oh-please do it right! This means the proper selection of two types of individuals; the proper in-depth linguistic training of the stenotypists; and matched, paired stenotypy training of the clerical people and of the scanner linguists. And also, have at least one of the monitors and developers of the program be a scientific linguist with the requisite knowledge of the possible pitfalls and difficulties. I am still convinced that a proper trial could well have positive results.

(C)

ANSWER TO "WHO & WHOM?"

(PAGE 4)

1.	Phineas T. BARNUM	&	James A. BAILEY
2.	Nathaniel CURRIER	&	James M. IVES
3.	Robert C. DUN	&	John M. BRADSTREET
4.	Isaac K. FUNK	&	Adam W. WAGNALLS
5.	William S. GILBERT	&	Arthur S. SULLIVAN
6.	Merriwether LEWIS	&	William CLARK
7.	Charles MASON	&	*Jeremiah DIXON
8.	Richard W. SEARS	&	Alva C. ROEBUCK
9.	Richard L. SIMON	&	*Max L. SCHUSTER
10.	Robert A. TAFT	&	Fred A. HARTLEY, Jr.

* The only two names in the right row.

And Harry says, "If you don't believe me, you can look it up in your Isaac K. & Adam W.!"

(U)

Letters to the Editor

P.L. 86-36

To the Editor, CRYPTOLOG:

[redacted] article in the July-August CRYPTOLOG ("Ye Gads! *Another* Country Trigraph System!") ends by asking if there isn't someone who can solve the problem he brings up -- proliferation of country trigraphs. I suspect that he is already aware that such a group already exists -- the NSA Data Standards Center (P13D). What he may not be aware of is that our group has no teeth, so we cannot force anyone to follow our lead.

The data standards problem that Jack brings out is actually only one of the many that plague this agency, as well as the whole U.S. government. As things stand now, we are not really in a position to know of many such problems until they are full-blown. Even the Senior Data Representatives, who are supposed to see all jobs before they are processed, too often find that they have been bypassed. Data files and data bases are designed and established long before we are brought into the picture and any attempts we make to correct errors are either ignored or circumvented. We have no power to make them change and they know that.

As the NDSC was first conceived it was supposed to have the capability for monitoring and investigating jobs to see if they varied from the norm. The NDSC would also have had the authority to take appropriate action if the initiator failed to conform to standards. For example, we would have been able to order the processing to be discontinued, or we could have denied access to computer systems to those programmers who were habitual offenders.

Yes, Jack, there *is* a standards center, but until we are authorized to deny computer use to those who refuse to accept Agency standards we can have little effect.

Mark T. Pattie, Jr.
Chief, NSA Data Standards Center

~~(FOUO)~~

To the Editor, CRYPTOLOG:

Dave Williams' NSA-Crostic No. 16 in the July-August 1978 CRYPTOLOG reminded me of the question I meant to ask when I read [redacted] Letter to the Editor in the July 1977 CRYPTOLOG, from which the puzzle quotation was taken. The quotation included the observation [redacted] I wondered then and still would like to know about the frequency in [redacted] of references to male traffic analysts. Perhaps some scholar has made a study?

Vera Filby, E41

(U)

To the Editor, CRYPTOLOG:

After several long hours of struggling to complete the July-August NSA-Crostic, distributed across many lunch periods, I was somewhat disappointed when I finally read the text that I had recovered.

Innocent as it may have seemed to Mr. Williams, I found it to be in extremely poor taste to perpetuate through this puzzle a bit of humor regarding female Traffic Analysts.

Although I now work as a Computer Systems Analyst, I have also worked as a Traffic Analyst and still consider myself to be a member of that profession. The quotation in the crostic is the type of statement that promotes basic prejudices that still exist in the Agency because they exist in our society.

I will laugh at jokes about female Traffic Analysts only when the opportunities for professional women are the same as they are for men, and when the rate of women promoted is equal to that of men promoted, and when the number of women in management positions is proportionate to the number of men in management positions.

Furthermore, until that time, the CRYPTOLOG will be doing an injustice to its professional quality by publishing such backhanded affronts to female employees.

[redacted] T323

(U)

ANSWERS TO **KNOW YOUR GEOGRAPHY** *(p. 6)*

1. *Libya*
2. *Cuba*
3. *Somalia*
4. *Venezuela*
5. *Austria*
6. *United Kingdom*
7. *Norway*
8. *Jordan*
9. *Thailand*
10. *Panama*
11. *Spain*

(U)

Solution to NSA-Crostic No. 17

By A.J.S. (CRYPTOLOG, September 1978)

[redacted] "[The] NSA Intern Program," *NSA Cryptologic Spectrum*, Fall 1977, Vol. 7, No. 4.

"The intern program was begun to provide an accelerated system through which new college graduates and in some instances experienced employees were trained to meet professional-level manning requirements."

(U)

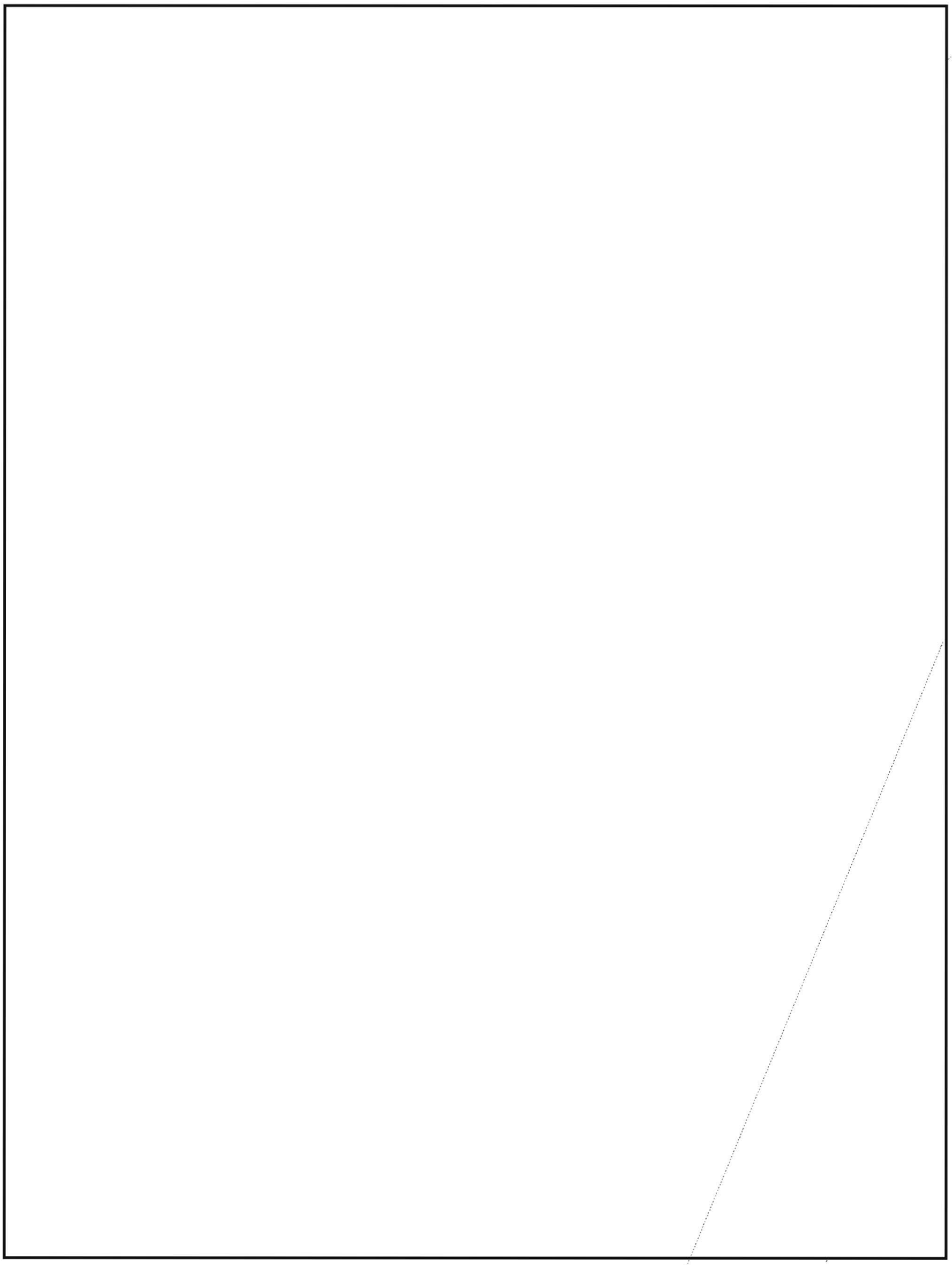
NSA-crostic No. 18

By guest NSA-crostician
David H. Williams, P16

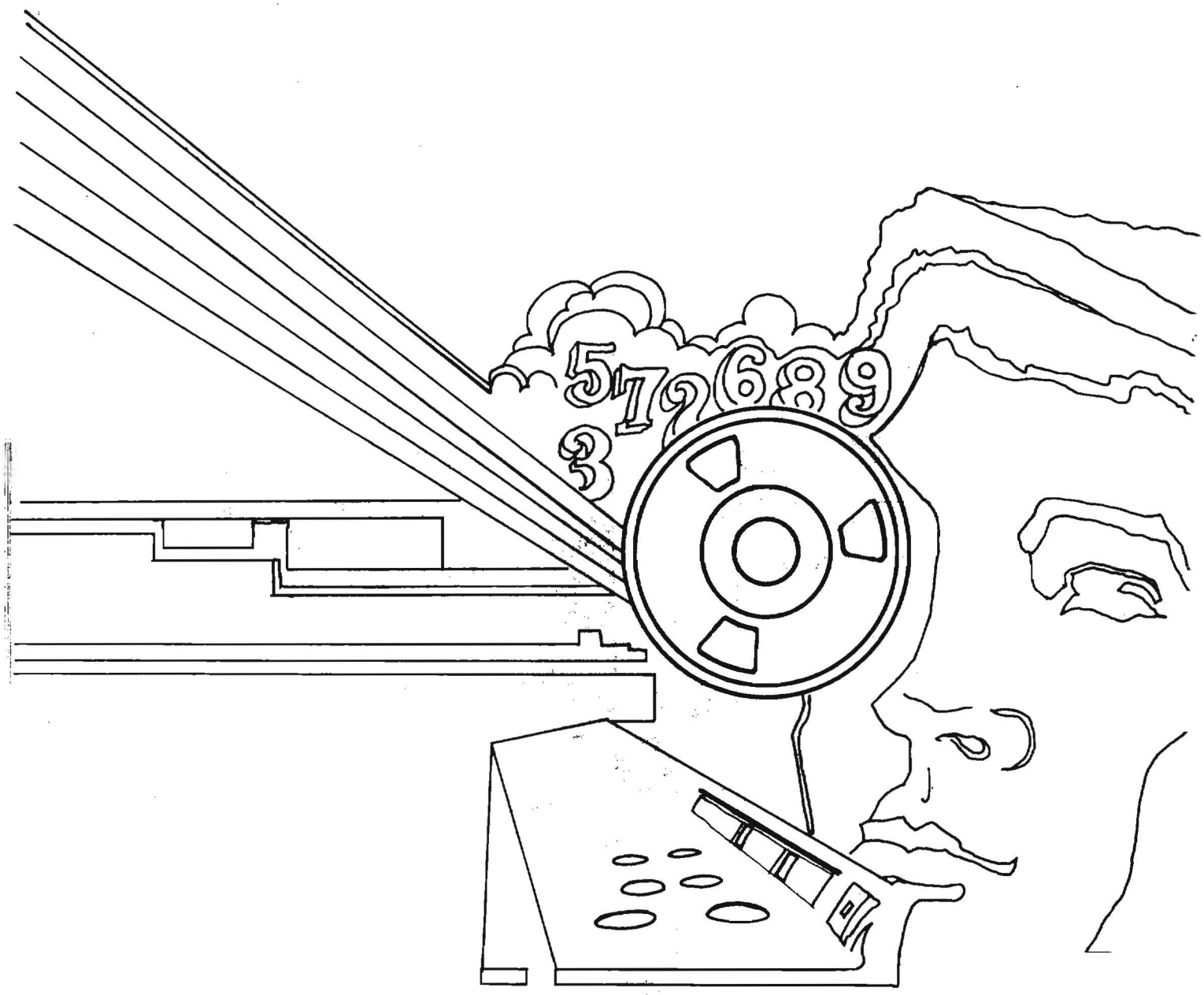
The quotation on the next page was taken from the published work of an NSAer. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS

WORDS



P.L. 86-36


5 7 2 6 8 9
3