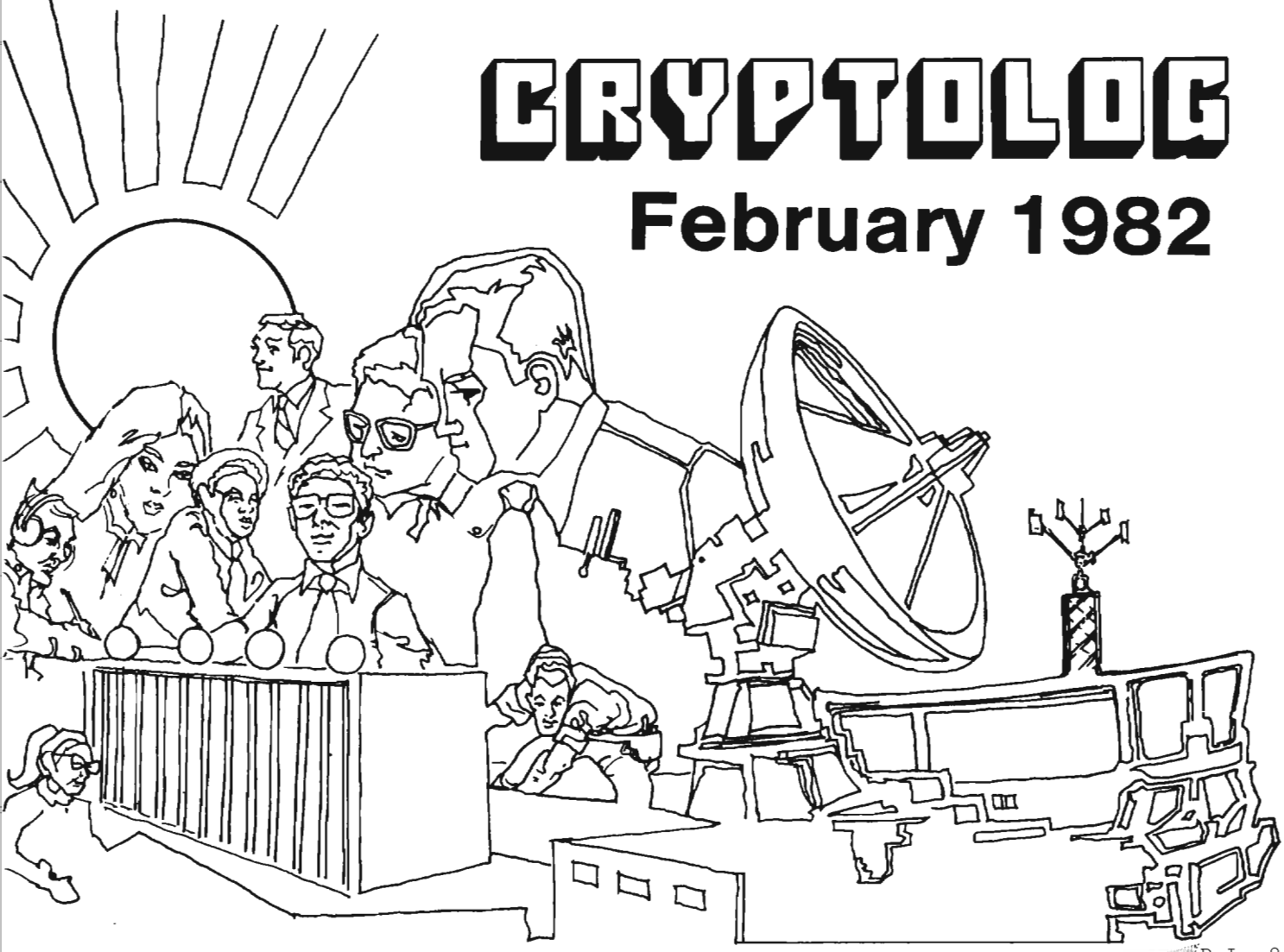
~~TOP SECRET~~

A27

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

February 1982



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 10 Feb 2012~~

CRYPTOLOG

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

VOL. IX, No. 2 FEBRUARY 1982

For individual (or organizational) subscriptions send name and organization

to: CRYPTOLOG, P1
or call [redacted] 3369s

To submit articles or letters via PLATFORM mail, send to

cryptolg at barlcØ5
(note: no 'O' in 'log')

Editorial

A man named Jim Wilson, from Moscow, Idaho, told a story the other day. It seems that a certain community had a high cliff that was the cause of repeated accidents. People kept falling off the cliff.

The town council decided to take action and passed a resolution to use whatever funds they had to buy an ambulance and keep it at the bottom of the cliff. One member of the council, who had been away on vacation, returned and questioned the decision. "Why don't we build a fence at the top?"

But he was overruled. "We decided to do this thing right! So we took a poll. Everybody who had gone over the cliff said they didn't need any fence -- what they needed was an ambulance. So that's what we bought!"

What are you working on -- a fence or an ambulance?

WES

P.L. 86-36

美繼續向台灣出售武

ประเทศเพื่อนบ้านใกล้เคียง

Native Scripting of Languages (U)

ปัญหาทางด้านเศรษฐกิจ

by [redacted] P16
MT/MAT Coordinator
In Collaboration with
[redacted] P16
Language Processing Coordinator

What is the value, in practical terms of providing an NSA linguist with worksheets in native script? This question has been asked and variously answered for as long as there have been NSA linguists. We may not be able to put the question to rest, but we hope here to surface the factors which need to be weighed in order to make an informed decision.

(U)

(U) The limiting factors in producing material in native script form are technological and economic. As technology has progressed, the availability of the script has increased, its quality has improved and the cost of producing it has decreased. By contrast, the linguistic and cryptanalytic reasons for or against having it have remained -- and may be expected to remain -- reasonably constant.

(U) What are the linguistic reasons favoring use of native script? They are so basic that no one would question them, were it not for the difficulties and expense of effecting the result. In the discussion which follows, ideographic languages, which pose the greatest challenge to technology, will be addressed specifically. However, general statements are intended to hold as well for other languages whose writing system is not based on the Latin alphabet.

[redacted]

[redacted]

(U) A second linguistic reason supporting native script is that almost all academic training is based upon it. Personnel arriving for duty are familiar with it, and those returning for advanced training must know it. Language acquisition requires extensive practice. Once learned, the skills are maintained through practice. If, after a thorough grounding, a person fails to use the language or some aspect of it, that person can usually reacquire the skills relatively quickly through practice, just as a person who once learns to ride a bicycle can, after a lapse of years, relearn the skill relatively quickly.

However, the person who has not learned the skill sufficiently well in the first place, whether it be riding a bicycle or reading a foreign language, will not enjoy this advantage of quick recall of skills. Providing native script routinely on materials processed daily gives the continuing practice needed to develop such a long-retained skill or to refresh a dormant one.

(U) The accompanying article was written in 1978 as part of the Language Processing Forum activities. The Forum itself is now dormant, but the remarks in the article seem to be current.

~~(C)~~ It is worth noting that NSA is now acquiring a hardware and software update of the IBM 3800 printing system. Included in the software package will be a set of dot matrix codes for Chinese, Forean, and Japanese, as well as an interactive character design program. Expected delivery date is 1 June 1982.

(U) Finally, the operational need for a flexible work force demands that a qualified language analyst in one element be readily transferrable to another element. As priorities shift or as attrition occurs within the work force, it should be possible to rotate an analyst with the appropriate language skill into another element, with a minimum of on-the-job training. Exclusive use of coding schemes by some elements and native script by others adversely affects this transferability.

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

[redacted]

~~(C)~~ The technological reasons for or against native scripts, as stated previously, change with the technology. There was a time when there were no automatic means for representing a large and complex character set. Since then, a wide array of offerings have been advanced, including cumbersome mechanical (impression) printers driven by paper tape; high-quality, high-speed plotters; and electronic devices such as full-graphics CRTs (cathode ray tubes) and electrostatic printers. Each component considered must be carefully assessed for its impact upon the analytic effort. The three major questions to be answered regarding adoption or rejection of a system are:

1. Are the characters of suitable quality for easy reading?

2. Will the system's dollar cost be excessive? and

3. What are the relative time costs?

These questions are subjective and should be made with as much valid information as possible. In answering the question regarding cost in money, the less tangible but very important linguistic impact, as delineated above, must not be discounted. In other words, the decision not to provide native script on the grounds of system costs must take into account the high cost of language training; the potential resultant decrease in the quantity and quality of SIGINT product; and the additional time, if any, it will take to train the language analyst in use of the alternative system. In a period when the supply of personnel with language skills is diminishing, collection technology is improving, and the work load is expanding, it is incumbent upon the manager to select methods which put those language skills to the most productive use. In regard to time costs, both the time delays imposed by the additional computer processing required to provide native script and the time enhancements accrued by increased productivity on the part of the linguist must be considered. Computer processing delays must be measured in conjunction with the time sensitivity of the problem and a conscientious assessment of the delay. For example, a delay of two hours could be excessive for a problem requiring 24-hour coverage and immediate response, while it could be quite tolerable for an operation being covered on one eight-hour shift, especially if the delay can be scheduled for a nonworking shift. Overall time enhancement resulting in more timely product may be expected when the technology selected for scripting does not inherently introduce excessive delays during prime duty hours.

[redacted]

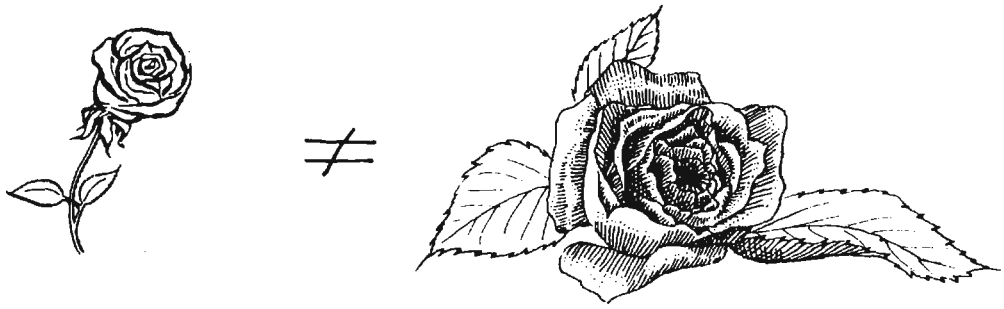
~~(C)~~ The following persons provided information which contributed to the report or concurred in the language of the final report (organizational designators reflect those at the time of concurrence):

[redacted] P.L. 86-36

A Time For Change? (U)

by [redacted] T53

P.L. 86-36



(U) With apologies to Gertrude Stein, a rose is not always a rose (at least not in the Intelligence Community). Over the years, each agency in the community (and many subordinate organizations) has developed and implemented its own unique formats for intelligence reports. Now we find that something as basic as the serial number by which a report is known has no common form, name or location. NSA calls it the "serial" but puts it on a line with no key; CIA calls it the "Report Number" and keys it accordingly; State Department calls it the "Message Reference Number" and puts it on the Classification line, while DIA calls it the "IR Number" and puts it in two places (the "Subject" line and the first line of Text).

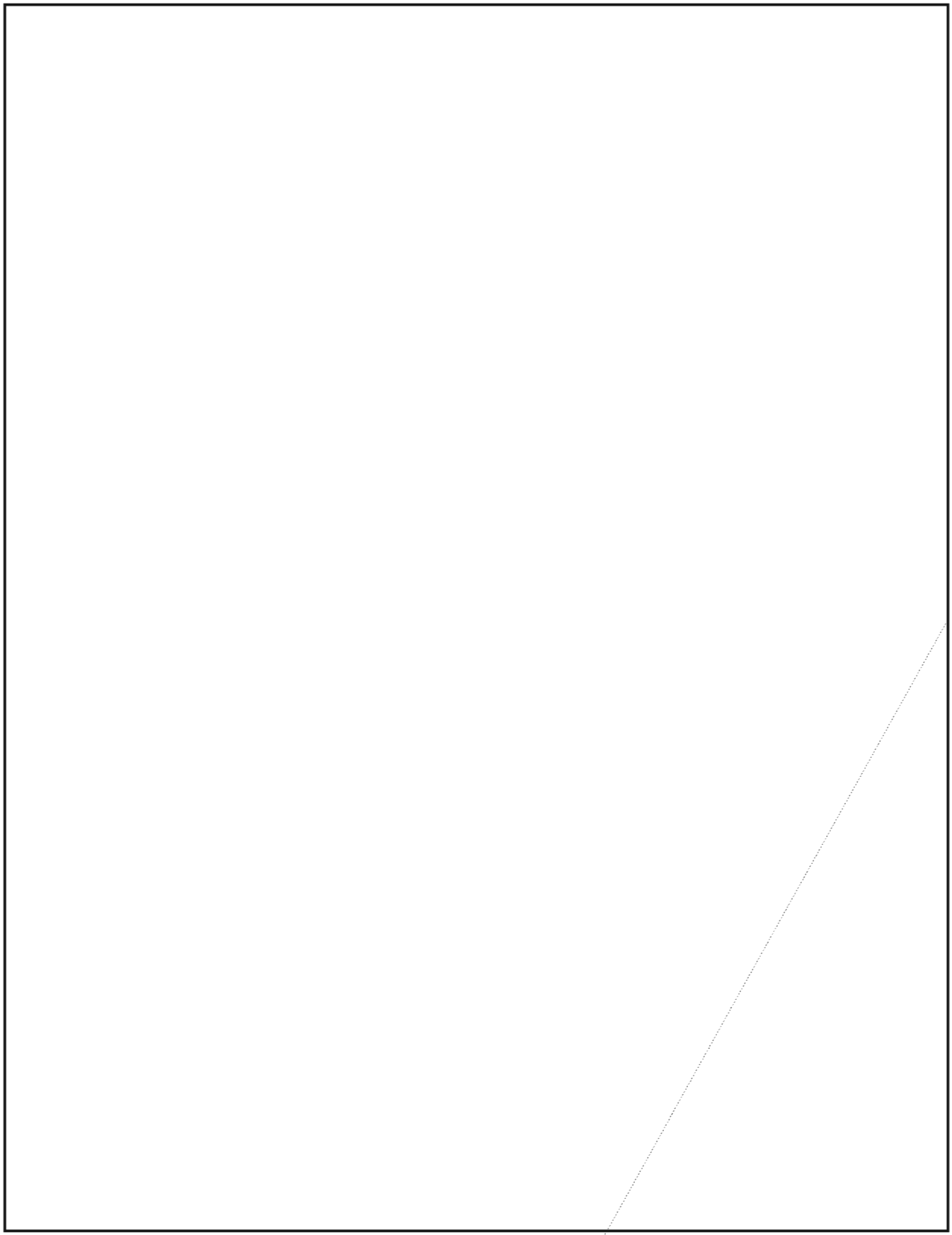
(U) Even within the same agency some vital report elements may vary from one vehicle to another. For example, the standard CIA electrical report has the report number in one place while the reports released by the Domestic Collection Division have the report number in two places (and often in modified forms). Also, the attention to format standards at the time of preparation leaves much to be desired in most agencies, including NSA. Key report elements are often misspelled, misplaced or arbitrarily abbreviated.

(U) Such "quirks" may have been inconsequential when everything was being scanned and distributed by hand. The human eye can easily search for and recognize whatever element of information is needed and will accomodate reasonable variations. However, now that each of the major agencies in the Community is building or planning to build major automatic distribution, indexing and retrieval systems, little differences add up to major design problems.

(U) The Intelligence Community is now at an important crossroad. The automation projects we are going to have to work with for at least the next decade are still in the development stages. If we are to resolve this format mess it must be now - before we are bound up by the implementation of systems designed for the individual formats. If not, each Agency will have to build complicated software to diagnose and index all of the report forms and the potential variations. Unfortunately, the increased complexity of such software will add operating overhead and require more human intervention in the form of editing.

(U) Any variation in the way similar elements of reports are presented adds significantly to the difficulty of retrieving information. If an analyst does not know that the serial number of a DIA Information Report is found on the Subject line, or that CIA reports contain a "Subject" not a "Title" he may well miss information vital to a project. Finally, if there is to be any significant sharing of bibliographic data bases throughout the Community, it seems reasonable that we speak the same "language."

(U) A study done by T5 of electrically received collateral intelligence reports revealed that, while there are unique elements in the reports of each Agency, there are also a significant number of common elements of information. Therefore a proposal to standardize electrical reporting formats was recently submitted to the Information Handling Committee (IHC) of the Intelligence Community (IC) Staff. The solution proposed is relatively simple; all members of the Intelligence Community should agree to and comply with certain broad format conventions for electrical reporting. This does not mean that all agencies will have to confine their



reporting to a single mold. Where there are common elements in the various reports, we should present them in a common way; and, where there are unique elements, we should use a standard pattern.

PROPOSED MODEL FORMAT (U)

(U) This proposal addresses only the information portions of an electrical intelligence report. It does not attempt to cover communications format problems. There are obviously, however, some areas that are of both information and communication concern. Where such an overlap occurs, an effort has been made to minimize the communications impact.

(U) In the proposed model format, the "information" portion of a report is broken into three sections: Address, Contents, and Management.

- The Address section consists of information about when the report was sent, who originated it, and to whom it was addressed. It includes the Precedence line, along with the From, To and Info lines.
- The Contents Section contains the body of the report, including the classification, accounting information, references, serial number, title, and text (among others).
- The Management Section contains information about the acquisition, preparation and disposition of the report. This final section would include review and declassification instructions, enclosure information, project numbers, etc.

(U) On the preceding page is an example of a DIA report in both the current and proposed formats. On the following page is a proposed list of the various lines that could be included in a report. No single report would ever contain all the lines listed as options, but every report would contain all those identified as required lines. Also included are examples of various other reports in the proposed format.

IMPACT ON NSA REPORTING (U)

(U) The IHC has formed a working group to look into the problem and make recommendations on the proposal. NSA, CIA, DIA, State Department, and each of the Services, have been asked to participate. T5, V1 and T1 represent NSA on this working group.

(U) The proposed format is not one used by any one Agency currently. It would require changes by all members of the Community, but represents a compromise employing facets from each of the current formats. No element of information being reported by any Agency would be omitted.

~~(C)~~ If the proposal is adopted as submitted, the expected impact on the current reporting format used by NSA should be minimal. We would flag certain lines with keywords (Serial, Accounting, etc), and probably change the Title to Subject. Other changes may be worked out by the working group as the effort progresses. However, since NSA has been reporting electrically for so long and using SOLIS for automatic indexing, our format is already well adapted to the current environment and is fairly consistent.

SAMPLE NSA REPORT

P 281906Z JUN 81
FM DIRNSA
TO NSA/OSCAR LIMA
[redacted] EO 1.4.(c)
NCR NMCC P.L. 86-36
WHITE HOUSE
BT

S E C R E T (CODEWORD) SECTION 1 OF 2
ACODEX/ ENP01F0081179
SERIAL: ?/XY/12345-81 SIGINT ALERT DUMMY
TAGS: ZDN ADEF AOPS LE SY
SUBJ: ZENDIAN AIR FORCE DEFENSIVE PATROL
REQS: TZ419

TEXT: _____
_____
_____

REVW: 28 JUN 11
BT
#3768
NNN

FUTURE DIRECTION (U)

(U) The proposal to the IHC also suggests that since format consistency and input quality are so important to the automatic indexing and retrieval systems, future on-line report preparation systems should be designed to do automatic quality control and verification of critical elements. In the case of NSA, we could have any product report being released checked by an abbreviated version of the SOLIS system. Thus, instead of editors correcting product reports after they are released, the reports would be returned on-line to the author prior to release with the errors marked. Obviously, such a system would have to have overrides for CRITICs or in the case of system failure.

Proposed Format

ADDRESS SECTION

** precedence/dtg
** FM
** TO
INFO
** BT or ZEM

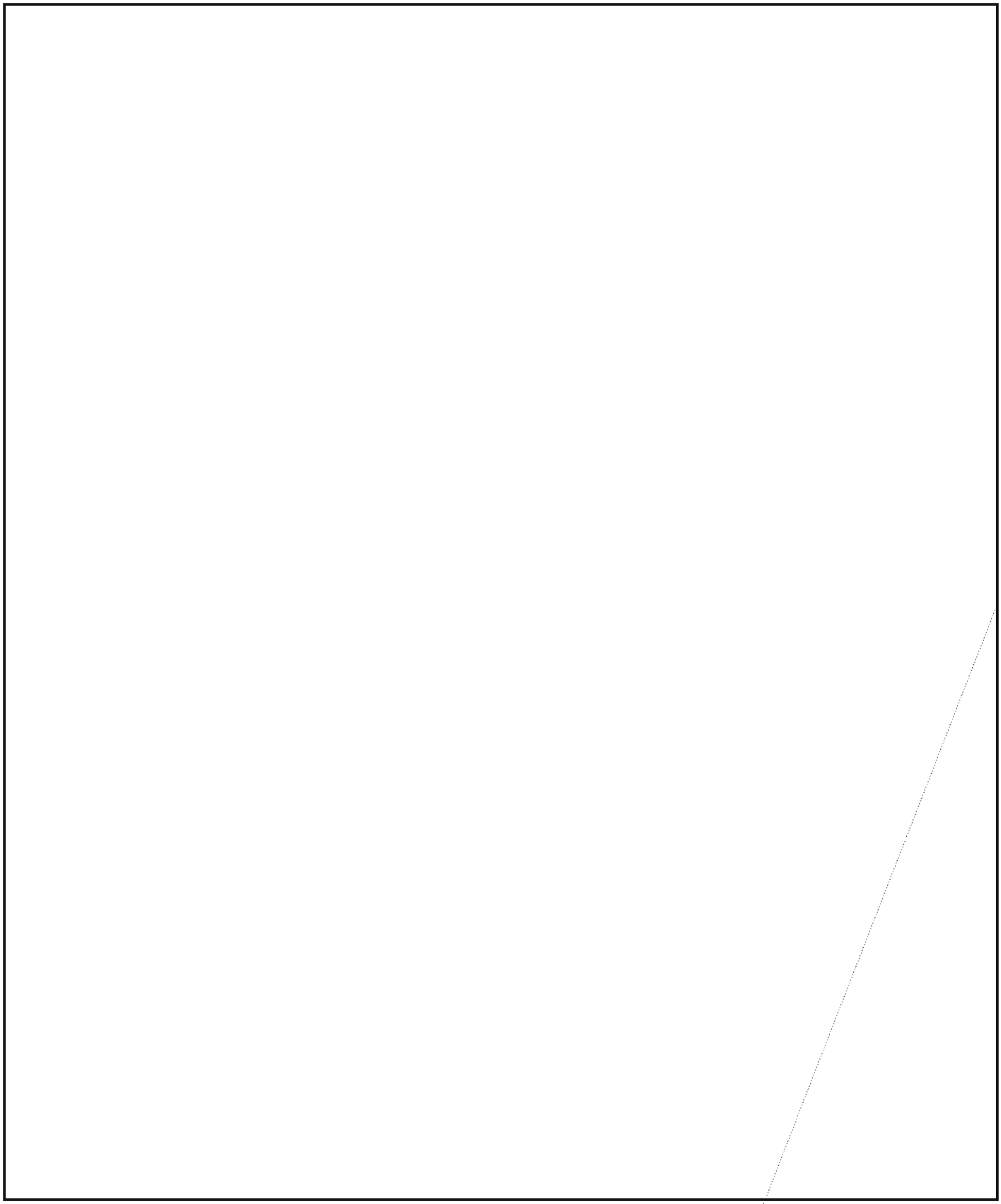
CONTENTS SECTION

**	classification/caveats	
	CITE:	Cite numbers
	ACODEX/	SIGINT accounting information
**	SERIAL:	Report number
	PASS:	Passing instructions
	WARNING:	Literal warning notices
	DIST:	Distribution date
	EO 12065:	State info on conformity with 12065
	CTRY:	Country codes
	TAGS:	Tag codes
**	SUBJ:	Title
	REF:	References
	DOI:	Date of the information
	ORIG:	Originator (other than the FM address)
	REQS:	Requirement numbers
	SOURCE:	Information concerning the source of the material
	SUMMARY:	Summary paragraph
	COMMENTS:	Preparers comments on the report
**	TEXT:	The actual body of the report (the Intelligence)

MANAGEMENT SECTION

	PROJ:	Project numbers
	COLL:	Collection management codes
	INSTR:	Special instructions
	PREP:	Prepared by
	APPR:	Approved by
	EVAL:	Evaluation requirement
	ENCL:	Enclosures
	ACQ:	Report acquisition information
	DISSEM:	Field dissemination
	REVW:	Classification review date
	DECLAS:	Declassification date
**	BT	

** denotes required fields

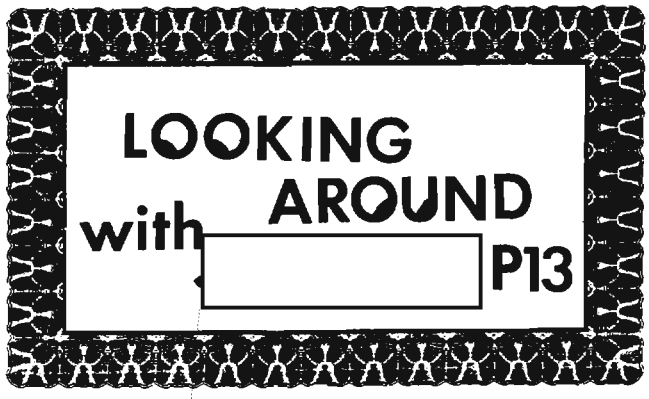


EO 1.4.(c)
P.L. 86-36

American Association for the Advancement of Science, 1982

◊Two Reports

- ▫ Software
- ▫ Gayler



P.L. 86-36

Programming languages and operating systems were analyzed from a human factors viewpoint in the 1982 AAAS (American Association for the Advancement of Science) meeting in Washington, by Dr. Ben Shneiderman of the University of Maryland. One of the surprising discoveries was that comments make a program harder to understand. Indentation also impedes understanding, which is opposite to popular belief. Most operating system messages are hostile, and accusing, e.g. FATAL ERROR, RUN ABORTED or ILLEGAL PASSWORD, as if the user had committed a crime. This apparently reflects an innate hostility toward other humans by systems designers.

An interesting technique was developed for controlled experimentation with programmers to test human factors. Programmers at some skill level were given a program to study which used certain combinations of language, comments, indentation, mnemonic names, control structures, etc. Then they were asked to reconstruct the program from memory. Independent variables were altered, and statistical methods used to verify hypotheses.

The cardinal reason why comments and indentation interfere with comprehension is that they take space and cause the program code to be spread over more pages. The page flipping impedes short term and long term memory, and creates "noise" in the understanding process. If the comments are printed to the right of the computer code, the resulting program script is much more compact. Indenting two spaces is better than four spaces. It is important to avoid dangerous cluttering. Higher level comments, which describe the problem domain rather than the program domain, aid comprehension. Shneiderman reported that the Begin-End blocks of PASCAL were harder to use than the When-If of ADA.

In the design of terminal operating systems there are three categories of users to be considered, viz. novices, knowledgable infrequent users, and experts. Each needs a different operating system. The novices need the utmost in clarity and simplicity, with a small number of meaningful commands. Knowledgable infrequent users need simple commands, which are easy to remember.

Psychological issues are:

- short term (human) memory load: the displays should be kept simple;
- closure, the desire for completeness;
- anxiety, called "computer shock" or "network neurosis" caused by the fear that the machine will dominate the user;
- locus of control, a desire to be in charge.

Response time is a complex matter. A lag of more than 15 seconds may disrupt thinking. Apparently it is beneficial to reduce the variation in response time within the system.

On line assistance may be more confusing than paper manuals. The screen formats should be predictable so the users will remember where to find information. Paper is a separate medium with wide bandwidth, non-volatile memory, portability and no outages.

Error messages are usually hostile, and frequently uninformative, e.g. "guard mode error 2". System messages should be brief, positive, constructive, specific, comprehensible. Usually the system messages are an afterthought, assigned to the least experienced programmer. The operating system should be designed around the system messages. Currently, no one keeps track of the errors that users make.

The mark of a good language or operating system is user satisfaction (not designer delight).

Shneiderman proposed that academic and industrial computer researchers should introduce controlled psychologically oriented experiments to develop research data on computer human factors. Commercial program and system designers should: create standards and metrics for software quality, develop guidelines for interactive system design, and promote the use of pilot studies.

Currently operating system "documentation" is word of mouth. It is efficient to write the documentation before the coding.

A number of publications were cited, viz: Software Psychology, a book by Shneiderman, and IBM Systems Journal. There was a six article series in ACM Computing Reviews, March 1981 on Database Language Research. At NBS in March 1982 there will be a meeting on "Human Factors in Computer Society".

McKeeman from Wang Institute noted that software was much too cheap and was produced by untrained amateurs whose low quality code caused expensive problems for the users. Programmers lack professionalism because they lack the power to say "NO!" to a bad task or decision. Programmers at TRW have about one tenth the training in their skill as GM auto workers. Where software is used in public safety matters, e.g. medical, air traffic, law enforcement matters, it should be produced by licenced professionals who can refuse to produce or certify inferior or untested code. (Note: the FAA is starting a $8.5 billion automated air traffic control system to replace most of the human controllers by computer software, so the issue is not academic.)

Stucki of Boeing observed that the direct cost of producing software may be much less than the indirect cost of the errors it makes. He cited the famous failure of the APOLLO 8 moonlander software which failed from input overload 30 meters from the moon's surface. The pilot then did a manual landing. Shuttle I was postponed for a software reason. The French have a system of 100 weather balloons, half of which were lost when the command software issued a self destruct order.

Irland of BTL said that 12 years ago the first SPC (stored program control) switch was designed for low down time, but failed due to severe software bugs that require reinitialization about 30 times a day, when a 40 year run between reloads was expected. The effects of real traffic were unforeseen. Now SPC switch software does not fail severely when it goes into service, but it still takes hundreds of switch-years of operation to discover and remove residual bugs. In 1950 BTL produced no software, while now 50 percent of BTL staff work on software. They now produce software at 100 times the rate of 15 years ago, but the team experience is lower.

There has been major growth in software effort, and in real time applications, and in life-critical applications (space, medicine, air travel). There has also been growth in the complexity of systems which network micros, minis and macrocomputers.

Maxims of software quality:

- Quality must be designed in, it cannot be tested in.

- Programs which are "good" or "correct" are of high quality.
- The earlier in the process the defects are eliminated, the better.
- Bugs are never all eliminated.
- The most costly bugs are in the requirements,
- There is a paradox in trying to control software quality when it cannot be measured.

A critical point is that all requirements must be testable. Many metrics for software quality have been found wanting. Some bugs are much more costly than others, so that mere bug-removal counts are not a guarantee of reliability. Initial bug density depends on requirements, experience of design teams, development environment, and methodology.

GAYLER ON ARMS CONTROL (U)

The elimination of manned aircraft, tactical nuclear weapons, chemical weapons, and small surface warships were among the recommendations made by Admiral Noel Gayler USN (Retd), former DIRNSA, at a AAAS meeting on Arms Control on 8 January, 1982.

The AAAS meeting was concerned with setting goals for defense R&D to improve the security of the U.S. and other nations. Admiral Gayler was joined on the panel by William Perry, former DDR&E, and Richard Garwin of IBM, a noted Arms Control expert. There was a surprising amount of agreement among the panelists about the uselessness of many expensive weapons systems, particularly the MX. Since Soviet manpower costs are only one fourth of their military budget, while these costs come to more than half of the U.S. defense budget, the point was aptly made by Dr. Perry that a numbers race against the USSR would be impractical because any expansion of numbers of weapons would increase the manpower demands and hence leave even less money for necessary hardware. Under Lanchester's Law, if the USSR has four times as many tanks, U.S tanks must be sixteen times more capable. This also is hopeless. The only answer to the Soviet threat, according to Perry, is the development of superior technology which doesn't require manpower or money.

Dr. Garwin criticized the MX and argued that the central problem in setting R&D goals was to search for better alternatives to unsuitable weapons. He drew attention to the bureaucratic and political obstacles to considering alternatives. He then described the SUM system, in which a fleet of small conventional submarines operate within 600 miles of the U.S. coast and carry a few MX missiles in capsules. The resulting secrecy and physical security would make a Soviet first strike impossible, and would cost much less than the MX. So far the Air Force appears uninterested in this alternative. Garwin advised looking for things that didn't fit into a bureaucratic niche, because new technology won't fit.

Admiral Gayler then developed his argument about new technology from first principles. The USSR and Warsaw Pact, he noted, had all the resources and physical means to maintain their war capacity already within their geographical domain. They had no global needs. The West by contrast was a loose transoceanic alliance. All the Western countries are in a deficit status in raw materials, they must import. China is a makeweight. There is no "China card" and no alliance. There are "uncommitted" countries, many of which have a surplus of resources. The national security missions in this context are complex, since economic and political factors as well as military factors apply. What do we want to do? The primary aim, according to Admiral Gayler was to avoid coercion by the USSR, i.e. where the USSR could split the US from its Western allies, or make the resources and raw materials inaccessible to the West.

The West can succeed in preventing Soviet coercion by concentrating its defense efforts, and reorganizing its defense, to try "leap-frogging" the Soviet numerical buildup and geopolitical expansion. The military tasks are:

- Keep sea and air communications open. This requires the capability to defeat air and sea forces, and to control information.
- Hold ground ,e.g. in Europe and Korea. The West must be able to defeat armor and infantry, and to control information.
- Project power in remote areas of the world, with or without bases.

To accomplish these goals requires weapons control. Enemy weapons must be hit precisely, not just bracketed by saturation fire. The effectiveness of modern precison guided weapons is great, and the total costs of an engagement will be reduced by accurate fire.

To illustrate the value of precision application of force, Admiral Gayler contrasted the mining of Haiphong harbor, which was accomplished without casualties and brought the North Vietnamese to the bargaining table to arrange a cease fire, with the combination of saturation bombing and massive infantry operations in the jungle, which were inconclusive and produced heavy casualties on both sides.

The new defense strategy would depend on modern target acquisition systems, imaging and signal processing, and detecting emanations. The primary applications of the new technology would be for the missions of search, surveillance and intelligence. Admiral Gayler noted parenthetically that most useable military intelligence comes from the electromagnetic spectrum, not from agents or informers. (Presumably this means SIGINT, imagery and radar). A central information "spider" with all data flowing into an overloaded central node for decision making, would not be suitable. Continuous control of information was vital. (Note: Admiral Gayler did not define the term "control of information" but apparently meant a broad concept of acquiring and protecting all kinds of information. Possibly he meant control of technological information as well as operational military information).

Space gives line of sight access for information and surveillance. Space will be the dominant factor in naval war in ten years, e.g. by the application of ocean surveillance systems and weapons guidance systems that will allow over the horizon targeting. The evolution of space to a combat zone is inevitable. Admiral Gayler gave the example of the early use of aircraft in World War I in which the French and German pilots on scouting missions waved to each other at first, but soon turned to battles for air supremacy. Space was a good place for a "contraption war" in which heavy battles between machines could be fought, without producing human casualties or collateral damage. To establish a U.S. military position in space the first step was to get a Space Commander, similar to the land, sea and air commanders now in control of those military missions.

Robotics will be an important factor in future defense systems. Current examples of robots are satellites and nuclear power plants, where complicated machines perform tasks in environments in which humans can hardly function. Manned fighter and attack aircraft are about obsolete in the current environment of surface to air missiles. Not only do the USSR and Warsaw Pact have a big SAM defense, but even small countries have SAM weapons which are capable of shooting down U.S. and allied manned aircraft. Admiral Gayler interjected a comment that although he was a former combat aviator, he saw no point to training and executing manned air missions in which the pilots had no chance of survival or of accomplishing their missions. The solution was to go to robot fighting vehicles on land and in the air. The man would be in the combat loop, but at a safe location on the ground, instead of being spun around at 6G stresses while he was trying to hit a target. Specialized small tanks, which were expendable and automated, could also do the ground combat function, with the operator safely located. The key element was a reliable data link, and Admiral Gayler was sure that U.S. technology could provide that. (Comment: if such remote fighting machines do come into service, future battlefield communications will be even more voluminous and critical than ever before).

Sea battles in the future will depend on acoustic warfare. At the present time the U.S. has developed its electromagnetic warfare and intelligence to a high degree. A similar development in acoustic surveillance, intelligence, countermeasures and security is needed.

People are a problem in the Armed Forces because there are too many of them, not used efficiently. Admiral Gayler said that, based on his experience as a task force commander, a modern large carrier could be operated with one half of the 2400 people, by better use of technology. He gave an illustration of a catapult operation, in which four men are used in a human chain to decide when to fire the catapult, which depends on the pitch and roll of the carrier, where one man with a reliable command control link could do the job faster and better. By reducing the size of the armed forces, the military services can be more selective in who they hire and retain. In training military personnel, the U.S. should use technology like the arcade computer games, rather than expensive and old fashioned training methods.

Maintenance should be based on "no failure" devices. Earlier, Dr. Perry had proposed "throwaway" maintenance, as currently practiced with handheld calculators.

Personnel policies in modern war should be based on motivation, selection and allocation of tasks. Admiral Gayler remarked that the main element in a sea battle was which side had the smartest Admiral.

Weapons of mass destruction have no military utility as theater or strategic weapons. If tactical nuclear weapons are used, the nuclear conflict will immediately escalate, and the damage to allies will be extreme. Therefore the only need is for central strategic nuclear forces, to deter any use of nuclear weapons, and these strategic systems should be survivable. The primary point of vulnerability in a central war is not the nuclear forces, but Washington itself. The USSR will develop and maintain both fixed and mobile ICBM's. Chemical and biological weapons have only a deterrent utility, they are not effective combat weapons.

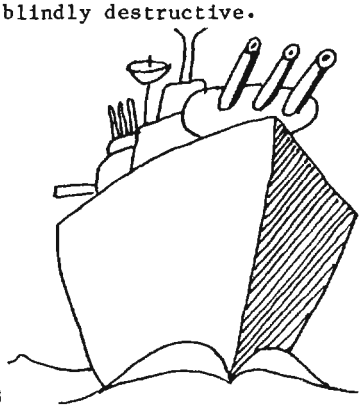
Money is important for defense, but currently most is spent on people. The answer is to reduce the number of people, not only in the uniformed services, but in the civilian bureaucracies which are associated with each Service, and have much duplication of staff and function. The elimination of the the three civilian Service Secretaries would, in Admiral Gayler's view, be useful.

Unneeded programs such as the B1, and MX should be cut. The B1 seemed to Admiral Gayler to have little use, while he stated that the MX was destabilizing. There is very little payoff in security from nuclear weapon development. Most of the surface navy is not needed, particularly destroyers. The Sea Control functions (of protecting shipping, and clearing or blocking sea lanes) can be done only by submarines, supported by long range aircraft and surveillance systems.

Science should concentrate on payoff areas, and should seek "step function" advances.

In response to questions, Admiral Gayler noted that the proliferation of precision guided weapons (PGW's) to small countries had raised the level of military violence in a way that could threaten US forces. His proposal for the elimination of all tactical nuclear weapons was predicated on reductions by both sides, rather than unilateral action. He agreed that the transfer of the Atomic Weapons program from Department of Energy to the Department of Commerce, which had no security role or competence, was not a sign of a well thought out reorganizaton. When asked about the apparent indifference of the "man in the street" to the massive and terrifying buildup of long range nuclear weapons, Admiral Gayler cited the psychiatric concept of "denial" in which a man told he has terminal cancer replies that he feel fine, refusing to even consider the facts of his condition. This, in Gayler's view, caused people to shut out the facts of nuclear annihilation, which are too awful to face.

When asked specifically what kinds of wars he thought the U.S. should prepare to fight in the future, Admiral Gayler said they should be non-atomic, should not involve large infantry commitments, and should be focussed only on specific military targets, like the mining of Haiphong harbor, which would be decisive rather than blindly destructive.



NSA-Crostic No. 38

by dhw

According to a long-standing show business tradition, a newcomer whose name is the same as that of an established performer must adopt a new name. Harry Morgan and Tim Conway are two examples of this tradition. Words M and V are two others.

A. Jayne Meadows' husband (full name)

265 140 119 97 184 168 128 133 180 200 215 65 189 75 40 95 233 161

250 145 171 5 83 186 49 197 109 31 227 220 202 158 19 18 89

B. ____ au rhum

84 199 25 195

C. Asian capital (2 wds)

92 244 108 4 157 166 257 231 105

D. See Word F (3 wds)

256 191 232 134 151 153 229 123 181 176 246 149

E. American singer and actor, former Rhodes Scholar and instructor of English at West Point (2 wds)

222 11 44 23 167 262 216 46 16 104 34 107 29 178 120 239 7

F. Play and film starring Word Q (3 wds foll. by Word D)

24 10 142 165 111 124 160 36 39

G. Hawaiian word denoting a non-Hawaiian person

88 59 209 72 68

H. Lap _____ (3 wds)

70 100 51 190 55 41 164 214 217

I. Customary practice

130 114 177 94 61

J. Spur, urge

77 87 169 125

K. Caribbean nation

15 129 174 183 156

L. Keen feeling for what is appropriate

110 81 172 115

M. British actor, real name James Stewart (2 wds)

154 173 50 147 20 91 192 1 207 45 76 14 185 196

N. Winner of 1981 Liberty Bowl (2 wds)

106 67 234 73 150 122 127 138 159

O. Delicate exactness, subtlety

228 137 113 144 9 162

P. Pierced with a sharp instrument

27 243 260 230 211 182

Q. Late American actor, former English instructor at Harvard (Thornton Wilder was one of his students), made his acting debut in Word F (full name)

264 117 253 206 226 212 99 193 21 112 28 245 6 241 240 ____

74 12 219 201 43 223 52

R. Percussion instrument

247 139 2 64 152 17 175 32 22

S. Tending to cause discontent or envy

T. Sleeveless garment; ness

U. Condition of being most satisfactory

V. British actress, real name Jennifer Jones

W. Sharp repeated rapping or knocking (comp.)

X. St. Francis of _____

Y. American actor, M.B.A., once employed by the Budget Bureau of Connecticut(2 wds)

Z. Made helpless

Z_1. "Too wise you are, too wise you be;
I see you are too wise for me."

255 131 143 238 170 248 148 116 102

58 236 204 57

47 63 35 258 80 224 235 132 66 146

8 79 53 60 187 86 259 252 101 136

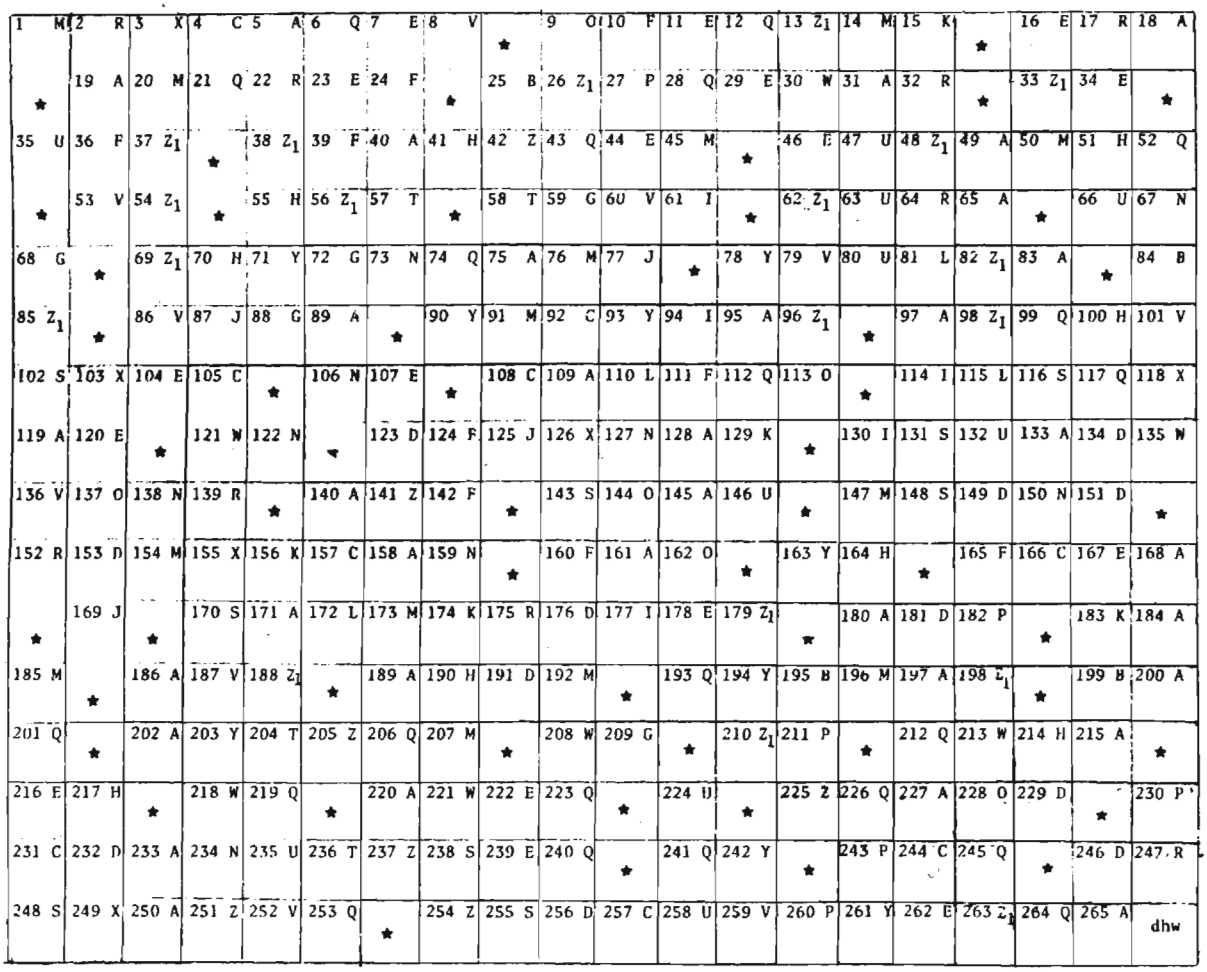
135 221 30 213 208 121 218

3 249 155 118 103 126

203 194 163 93 78 242 261 71 90

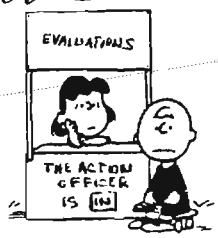
141 42 225 237 251 205 254

179 54 13 96 198 85 62 210 263 48 26 82 188 56 69 33 98 38 37



The Internal Performance Evaluation: *Friend or Foe?* (U)

[redacted]



P.L. 86-36

(C) What do the USSID System, the Alternate Intercept Coverage Plan, the Vital Records Program, and Agency Staff Responsiveness have in common? As you may have deduced from the title of this article, each is the topic of a recent Internal Performance Evaluation -- IPE, for short. It is readily apparent that IPE's cut across a wide spectrum of Agency operations; so, it is probable that you will one day encounter the process. In this article we hope to take the mystery out of the IPE by defining it, by examining how it comes to be, and by looking at the results that come from it. In so doing, we hope to convince you that the IPE is not a foe, but a friend -- a friend that has the potential to improve your operation.

(U) To begin, we should put the IPE into its proper perspective. The IPE is one of several elements of the Performance Enhancement Review Program (PERP). Established by USSID 520, the PERP is a management system designed to provide DIRNSA/CHCSS, Key Component Chiefs, and SCE Commanders with information needed to make decisions concerning the operational performance of the US SIGINT System. The objective of the PERP -- and consequently the objective of an IPE -- is to improve the efficiency, economy, and effectiveness of the US SIGINT System.

(U) The Director of Performance Evaluation manages the PERP, which includes not only the IPE's but also Field Assistance Visits, Field Evaluation Visits, and a PERP Panel. Overall, the PERP examines systems, programs, plans, or activities that support the US SIGINT System. Specifically, the IPE evaluates systems, programs, or activities internal to NSA and under the direct operational control of DIRNSA/CHCSS. The PERP Panel, an executive forum for coordinating and evaluating results of the PERP, may be used to discuss potential IPE topics, the status of an ongoing evaluation or the results of a completed one.

(U) How does an internal Agency program or activity become the subject of an Internal Performance Evaluation? It begins as a proposal from Congress, DIRNSA, Key Component Chiefs, SCE Commanders, or individuals assigned to the Agency or to its field activities. Many of the proposals, however, are generated within the Performance Evaluation Directorate itself, Q2.

(U) The proposal process begins by defining a potential internal evaluation topic and ends with a management "go/no-go" decision. There are two major decision points along the way. The first of these is the evaluability assessment. A potential topic is assigned to a research Action Officer, who first validates it through a cursory examination of the topic and the variables involved, and then makes one of three recommendations:

- to continue the evaluation,
- to terminate it, or
- to put the proposal into a data bank of projects to be conducted at a later date.

The decision at this point is made by the DPE.

(U) If the decision is to continue the evaluation, then the Action Officer will conduct detailed research, meet with concerned activities or elements, and conduct briefings or meetings as required. While doing research in-depth, the Action Officer also develops the evaluation methodology, the road map that will be used to reach the most valid and reliable conclusions within available time and personnel constraints. The methodology developed is a large part of the second major decision product, the formal Evaluation Proposal.

(U) As you might expect, the Evaluation Proposal really digs into the topic. It looks not only at the methodology, but also reviews the background of the subject and tries to assess what contribution can be expected when the evaluation is completed. It defines the approach to the evaluation, explains what data will be collected and how it will be analyzed, and tries to estimate the cost of the

evaluation. The objective is to help management decide whether the proposed evaluation is both feasible and worthwhile.

(U) If you have the impression that the Evaluation Proposal process is time-consuming and methodical, then you are correct; but we keep it that way for good reason: we don't want you to view the IPE negatively. In fact, we think the most important parts of the proposal process are the communicating and coordinating that go on. At every step of the way, the Action Officer and the elements involved work together. They participate in meetings and briefings on the topic, and they jointly develop alternatives, options, and recommendations. All this is to ensure the integrity of the evaluation and that it works *for* you, not *against* you.

(U) Here, perhaps, is the proper point to underscore our relationship with the Inspector General (IG). Simply put, we are not an IG; we do not function as one; and we do not do their staff work. We do not, as a matter of course, coordinate all our proposals through the IG. If, however, our workup of a topic leads to an area where IG involvement is appropriate, then we must coordinate our efforts with them. For example, fraud, waste, and abuse are currently high-interest areas in the Federal Government. Should an example of fraud surface during a proposal process, then we would be remiss if we did not act to bring it to the attention of the IG. In fact, this has never happened; but if it did, we would certainly make sure that the action was fully justified and that the organization being evaluated was fully aware of the situation.

(U) Once an Evaluation Proposal is approved -- and depending on the nature of the topic, we may go all the way to the Director with a Decision Memo -- the implementation process begins. First, a Team Chief is assigned to the evaluation. This may be the same person who developed the proposal, but that is not always necessarily the case. It is entirely possible, for example, that one Action Officer would do the proposal and another perform the evaluation itself. The Team Chief, together with the management and technical experts already identified, begins the data collection, reduction, and analysis process. Whatever format this takes -- questionaires, statistics, interviews, etc. -- the methodology is followed to end in a draft report. The draft report is coordinated first with the team members, then through Q2, and finally is distributed to appropriate elements Agency-wide for review and comment.

(U) The IPE Team collates all external inputs and incorporates them into the final report. It is important to note that the report will make every effort to present all points of view. Of course, there may be occasions when some opinions must be abridged or omitted from the body of the report. In these cases, they will be appended to the background material forwarded with the final report for management consideration. The report usually does not stand alone; rather, a briefing accompanies it. Yet, even then the process is not complete. Each report leads to conclusions and recommendations, and the task falls to the Team Chief to monitor the implementation of the approved recommendations until each has been resolved. In this way, we try to ensure that an IPE is not a "one-shot" action, but a continuing process that leads to a system improvement.

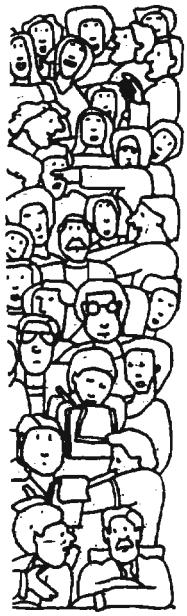
(U) Suppose that you would like a problem evaluated, but you do not want a detailed, formal evaluation. Or perhaps, you would like to conduct your own internal evaluation, but do not know exactly how to start. Q2, as the NSA/CSS central authority for coordinating Agency performance evaluation activities and conducting performance evaluations, will be happy to assist you on either a formal or informal basis. We have a staff with a variety of backgrounds and experience in SIGINT and COMSEC operations as well as engineering and operations research skills. We are prepared to offer assistance in any way that will improve efficiency, economy, and effectiveness.

(U) To recap, IPE's are a management tool that can be applied to any aspect of internal Agency operations. IPE topics can be suggested by anyone and they all follow a structured path through the evaluation and implementation processes. Each step of the process is so designed to preserve the integrity of the evaluation and to make of it an exercise in participative management. The principles of coordination and collaboration work to ensure that the Performance Evaluation Directorate is not perceived as an IG. The entire process is usually lengthy and always methodical, the better to guarantee that the results will contribute in a positive manner to the effectiveness, economy, and efficiency of the US SIGINT System.

~~(C)~~ So what do the Afghanistan Crisis, the Russian Language Acquisition Program, and NSA's Emergency Destruction Capability have in common? Like the topics listed at the start of this article, they have reaped the benefits of an objective evaluation process, the IPE.

(U) If you have a problem that you think would benefit from a formal or informal evaluation, contact Q2. We will be happy to assist you.

A Wail, A Complaint, and a Melange (U)



by Samuel S. Snyder, T54, et al

Editor, CRYPTOLOG:

Herewith a couple of poetic contributions by former associate, the late Captain William M. V. Hoffman. Bill was assigned to my section, "B-II-b-4-a" sometime in 1942, when we were first becoming successful in our attack on the Japanese Military Attache system. Bill was a former Episcopal priest who was distantly related to Franklin D. Roosevelt, and liked to tell of having breakfast at the White House with FDR. He had an uncanny knack with words but somehow had a terrible time making good guesses when we assigned him to overlap work. His frustrations come through in his "Wail of a Cryptanalyst." We made good use of his talents later when we assigned him to write training materials for new people coming on the job. In his "Arlington Melange" you might have fun trying to identify individuals he had in mind on each line. (Example: the "genius dashing about like a flea on a binge" is Frank Lewis!)

The other poem about computers (*by* a computer!) was started by me on a plane late at night, while flying home from a computer conference in Detroit, in 1951. By the time we landed, I had about five or six verses; the rest were composed the next day in the office, including contributions by Red Lathroum, John Rixse, and Dotty Blum.

Samuel S. Snyder, T542

ARLINGTON MELANGE (U)

by William M. V. Hoffman

There are M.A.'s from Harvard and Princeton,
Musicians and doctors of law;
    There are all kinds of teachers,
    And even some preachers,
and pale-faced Ph. D.'s by the score.

There are anthropological experts,
And Swedes who are silent and bland;
    And one of our bosses
    Is a colonel of horses
Who longs for an active command.

We have graduates straight from Smith College
Who are brilliant and friendly and fair;
    We have mathematicians
    And bright statisticians,
Who can calculate odds to a hair.

There's a plentiful sprinkling of screwballs,
And a few on the lunatic fringe;
    While temperament flashes
    And genius dashes
About like a flea on a binge.

We're a weird and outlandish collection;
We're a cockeyed and comical crew;
    But, come Nazis or Japs,
    You'll find we're the chaps
Who will see that the message gets through!

THE WAIL OF A CRYPTANALYST (U)

by W. M. V. Hoffman

There are moments when the world looks bright
and rosy,
When the messages are tailing as they should,
When each fancy little letter
Makes the columns come out better,
And the rows could act no better
if they would.

Then the heart of the cryptanalyst is merry,
And he chortles as he sets the traffic down;
And he thinks the enemy chaps
Are such simple-minded saps,
And the man who makes their ciphers is a clown.

But, alas! there comes a day of horrid failure;
Our cryptanalyst is miserable and blue;
And the nasty little letters
Thumb their noses at their betters
And make gibberish no matter what you do.

You can stand them on their heads
and read them backwards,
You can shift them left to right
and to and fro,
You can calculate and mutter
Till your brain becomes like butter,
But no matter what you try it doesn't go.

Then you curse the day when ciphers
were invented,
And you kick yourself around for being dumb;
And the guy who once invented
Such a code is a demented
Low-down, slinky, lousy, dirty, rotten bum!

P.L. 86-36

COMPUTER'S LAMENT (U)

by [redacted] and Friends*

(March 1951)

My business is computing
With great efficiency,
Though what it's for is more and more
A mystery to me.

My heart beats are electrons,
My mem'ry works quite well;
But where I go or what I know--
That, only man can tell.

My rate's a megacycle,
My cost - a megabuck;
But if I make just one mistake,
My friend, you're out of luck.

My names are always silly,
With "Ack" they often rhyme,
Be dignified, I've got my pride,
Let's joke some other time.

My mem'ry's like an elephant's,
Each number sticks like glue.
I don't regret what I forget--
I'm filled with something new.

When coders misinterpret
My numbers, new and old--
It's all the same, I get the blame
For doing what I'm told.

The people all around me
That come and go each day--
Sometimes they fuss, sometimes they cuss,
Sometimes they sit and pray.

The operator ponders,
The coder strokes his chin;
But Oh! the loud annoying crowd:
They stand around and grin.

My ills are well attended,
My docs are maintenance men;
Oscilloscopes and lots of hopes
Can fix me up again.

My access time can vary,
Whatever they decide;
But fast or slow, they still say "No!"
They're never satisfied.

Sometimes I am disgusted--
Sometimes there is no joy;
For I can see that I will be
A million dollar toy.

Sometimes I get quite weary
While pulsing through the night;
But if I err, just hear them swear!
They never treat me right.

They don't appreciate me
In spite of all they say;
Why, I do more than fifty score,
And, brother, that ain't hay!

So feed me lots of power,
Adjust my settings right;
And if we try, then you and I
Can help to win this fight!

* Dorothy Blum, Leo Lathroum, John Rixse

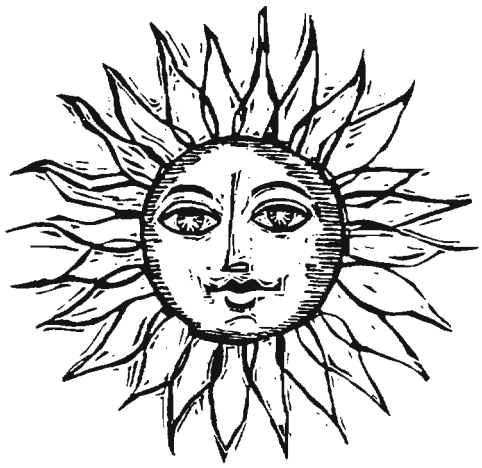
KRYPTOS:

A New Society (U)

by [redacted]

P.L. 86-36

CA Intern,
KRYPTOS Society
Historian



(U) The KRYPTOS Society, chartered in October 1981, is a new organization whose purpose is to promote cryptanalytic excellence and to provide a focal point for Agency cryptanalysts. On 9 December 1981, at the Society's inaugural meeting, Miss Ann Caracristi, Deputy Director NSA, spoke on 'Cryptanalysis: the Key'. Her address was followed by comments by [redacted] on the steps taken by the Cryptanalysis Career Panel, of which he is the chairman, toward 'restoring the luster to cryptanalysis'. Attendance at the meeting was outstanding. In the interest of accurately recording the comments of both speakers, this summary has been prepared from notes taken at the time.

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

~~(C)~~ Miss Caracristi observed that without cryptanalysis there would be no National Security Agency, yet there existed no CA organization until 25 years after the founding of the Agency's first professional society, the CMI. She then addressed the problem of identifying Agency cryptanalysts. Everyone, it seems, knows what a cryptanalyst does but no one knows just what one is. The mathematicians in the back rooms of A5 and G6, are they cryptanalysts? What about the signals people in A5 and B3? And the linguists of G6, A2, and A3? They all perform cryptanalytic functions; aren't they cryptanalysts?

~~(SC)~~ Whatever your definition, several names come to mind as eminent cryptanalysts: William Friedman, Frank Raven, [redacted], Peter Jenks, Bill Lutwiniak, [redacted], Phil Dibben, Jim Thompson, [redacted] These and many others have, through their successes, saved countless lives with the information they provided -- breaking ENIGMA and PURPLE in World War II, providing tactical decrypts during the Korean Conflict (1950-52), and maintaining successful efforts against the Viet Cong. [redacted]

P.L. 86-36

~~(S-CCO)~~ But with success, Miss Caracristi pointed out, problems arise. Exploitation leads to production and we find ourselves making less of an investment in new problems. The number of cryptanalysts (including crypto-math) has shrunk [redacted] Success also has an impact on other fields. It creates work for the linguist, the engineer, and data systems person, and the collector. And, as a [redacted] Miss Caracristi put it, "The alarm bells are ringing."

~~(S-CCO)~~ The KRYPTOS Society can help the CA work force by

[redacted]

- providing support to the CA Career Panel,
- identifying new talent for the CA work force,

- providing mentors from its membership for new cryptanalysts,
- keeping up with events in the outside world and in the academic community, and
- advising the Director on the health of the profession.

~~(FOUO)~~ Miss Caracristi concluded her remarks with the following words of guidance:

> We should look to the immediate future as an opportunity to recapture CA manpower through recruitment. We must bring new cryptanalysts on board and develop their CA abilities, teaching them to appreciate the excitement and the challenge of tackling hard problems, to learn to enjoy small successes and to follow their intuitions when the trail gets hot. By doing this, we can build for NSA's continued success.

P.L. 86-36

(U) When [redacted] became chairman of the Cryptanalysis Career Panel two years ago, his goal was to restore the luster to cryptanalysis to counter losses the field had suffered. Toward this goal, he set three objectives:

- ☆ to provide a place for middle and senior cryptanalysts to seek advice and to learn of potential in other organizations; an informal, nonthreatening resource for post-professional career development,
- ☆ to establish a professional society for cryptanalysts, and
- ☆ to establish a technical excellence award for the field of CA.

(U) The first objective was a service that could be provided by the Executive of the Cryptanalysis Career Panel, since the Panel's responsibilities included much more than training interns. Over a period of time, the position of Executive of the Panel had been downgraded from its initial grade of GG-15 or GG-16. Elements of 'M' were proposing that the Executive should be a grade GG-12. Mr. [redacted] was successful in getting them to upgrade the position to a GG-15 once again, a grade level more appropriate to the broader duties of the office. At this time, [redacted] became the Executive, eventually to be succeeded by [redacted] then talked with office chiefs and obtained their endorsement for regular visits by the Executive to CA offices to see what was being done and what was not.

(U) One deficiency noted by the CA Panel was the lack of a professional society for the central profession of NSA. They weren't sure of the level of interest in such an organization, but knew of the tremendous popularity of CA-305, an annual seminar series. To determine the amount of support such a society might expect, questionnaires were sent out. Encouraged by a good response, the Panel formed a committee to organize the society that eventually received the approval of the Director and of the Council of Learned Organizations.

(U) In establishing an award for technical excellence in the field of cryptanalysis, the Panel wanted to recognize steps taken along the path to success. Frequently those at the end of the road are recognized while early contributions go unrewarded. Additionally, recognition often depends on the value of the output. The Panel wanted to recognize 'coups of the mind' without regard to whether or not vital decrypts were produced. The award was envisioned as a pin with the possibility of a plaque for two-time winners. Nominations would be accepted as events occurred. The Panel would act semi-annually to select recipients, presenting perhaps ten awards per year.

restoring the luster to cryptanalysis

(U) The award was originally conceived by [redacted] as an Agency award. When he took the proposal to [redacted] then DDM, Mr. [redacted] suggested that to establish it as an Agency award would take a long time and a great deal oof red tape. Offering it as a professional society award, however, would be relatively easy. With this recommendation, the award was put on a back burner until a professional organization could be formed. Eventually, DDM became DDA and [redacted] was replaced by [redacted] When [redacted] made a point of acquainting [redacted] with the proposal, he was advised that it shouldn't be a professional award but an Agency award. Having waited this long, [redacted] resisted changing the proposal again. With the establishment of the society well on its way, Mr. [redacted] made an appointment to discuss the new society, the award, and the objectives of the Panel with Director Inman and Deputy Director Caracristi. Admiral Inman, on hearing of the award proposal, expressed a strong opinion that it should be an Agency award. Strong opinions at that level are always considered. When the M34 Awards Division was approached with the award proposal, they recommended that it should be a professional society award, not an Agency award! It was then that [redacted] did a little name-dropping, apparently convincing them that an Agency award was entirely appropriate.

(U) Establishment of the award was then hung up in the legal office for over three months. The Panel, meanwhile, to decide on a name for the award, went to Q23 with their original suggestion, 'Excellence in Cryptanalysis'. But Q23 didn't want any reference to CA in the title. They wanted to avoid identifying our best cryptanalysts to the outside world and expressed concern that the design of the pin might be too revealing as well. And in addition to the legal office and Q23, the offices of Protocol and Heraldry had become involved. [redacted] had been correct in his appraisal of the situation.

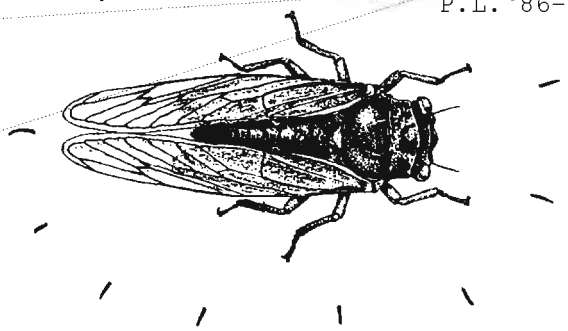
(U) [redacted] tasked by the Panel with choosing a design and name for the award, suggested the 'Gold Bug Award' after Edgar Allen Poe's story involving the breaking of a cipher. This suggestion solved both the name and design problems -- the name did not refer to cryptanalysis and suggested obvious design ideas. The award proposal is now in the 'M' office that provides documentation on the administration of such awards. [redacted] expects the award to make its appearance sometime in 1982. The Panel proposed that nominations go to the CA Career Panel, who would decide on the recipients. In closing, [redacted] offered his favorite maxim for NSA cryptanalysts:

"The impossible we do immediately,
the miraculous takes a little longer."

(U) The KRYPTOS Society welcomes new members. For information, please contact any of the following people:

President	[redacted]
President-Elect	
Treasurer	
Secretary	
Members-at-Large	
Program Committee	
Membership Committee	
CA Panel Exec	

P.L. 86-36



Correspondence

From: tfh at CARONA
To: cryptolg at BAR1C05

Wayne,

(U) I received the message sent to Unix users back in October and I am taking this opportunity to express my feelings on the subject of communications of the users on these systems.

~~(FOUO)~~ Having worked in the [redacted] TSS area for several years, I have had the pleasure of working with a number of people, who use the Unix Systems. There is truly a wide range of people using the systems today and an even wider range of tasks being performed. No one has the time or the need to use everything on the system; each individual specializes in some particular area which fits his or her own personal needs. Each day someone discovers a new method of improving that area. The users manuals help with the basics, but it would be impossible to document all the routines and working aids that people have perfected and used on the systems.

~~(FOUO)~~ In the past, I have attended several meetings of UNIX-BASED TERMINAL SYSTEMS USERS GROUP. The purpose of these meetings is to give users information on developement of the Unix systems and to stimulate interest in areas which users are having problems. The trouble with the meetings now, I believe, is that they are aimed at the Systems programmer level rather than at the user level. A majority of people who attend these meetings are Systems people themselves or deal more with the programming applications of the system. The material presented is on a level that is hard to comprehend by those who are not programmers themselves.

~~(FOUO)~~ You stated in your message "I only ask that the material be sufficiently readable so that people who don't work in your special skill area can read it through and come away with some appreciation of how things are going in your territory." I feel that everyone working on the Unix systems has some territory in which he has extended use, where he might share his specialty with others, who may not be as versed as he, in that particular area.

~~(FOUO)~~ Perhaps, then, we UNIX users should start talking to each other and start sharing our ideas. Indeed, Cryptolog itself might serve as a useful vehicle. We have the resources available to us already, so "Why re-invent the wheel?"

[redacted]
T1512

P.L. 86-36

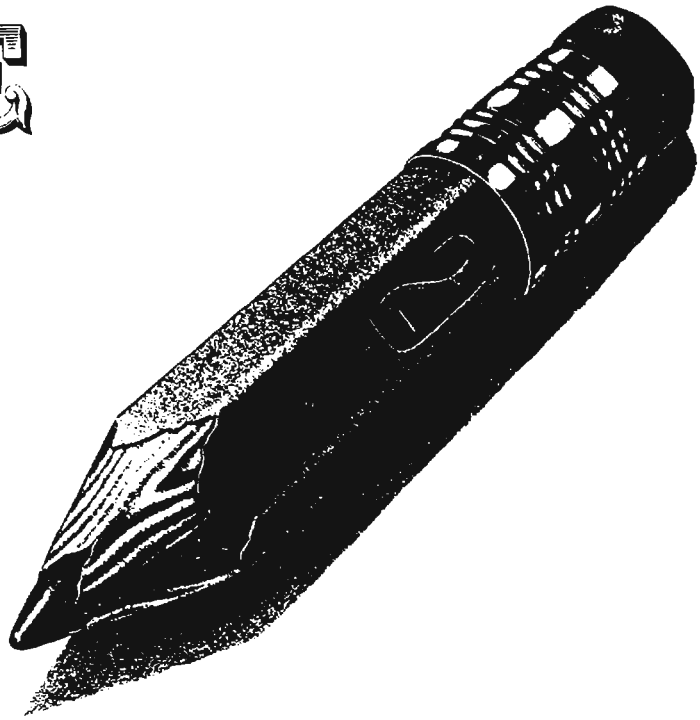
SOLUTION TO NSA-CROSTIC No. 37 (U)

"Language in the News," [redacted]
[redacted] CRYPTOLOG, September 1974

"The Wisconsin Native American Languages Project is an undertaking funded by the Great Lakes Inter-Tribal Council, to involve speakers of Wisconsin Indian languages (Ojibwa, Potawatomi, Menomini, and Odeida) in the application of linguistics to the analysis, study, and teaching of [these] native languages."

(U) RYE is scheduled to be phased out by mid 1983. Efforts are under way to get in touch with all users. If you are an active user and have not been contacted by now, please advise T1533, extension 4030s.

GOLDEN OLDIE



Simplicity in Color

by C. Garofalo

(from COMMAND, October 1971)

The conduct of crypto TA studies involves the requirement to differentiate between qualitative levels or categories, and the use of a simple color scheme facilitates such differentiations. Any color scheme to be used in an analytic effort of large volume must be:

- simple in nature,
- skillfully chosen, and
- systematically applied.

An analysis of the various colors available is made to determine which are practical and most suitable for the task. My experience has demonstrated that six different colors are most practical. These are black, green, red, blue, purple, and brown.

- Black - carbon (number 2) pencil has been found to be the obvious choice for normal usage. It is of a medium degree of hardness and density, suitable for both erasure* and longevity properties.
- Green - is the weakest, that is, of lightest density. All of the other colors under consideration superimpose on green quite readily.

* For black erasures, a medium hard rubber erasure is adequate. For color erasures, best results are obtained with a typewriter eraser.

- Red and Blue - are of equal boldness; either can be easily superimposed on both black and green.

- Purple - a bolder color which can also be produced by a superimposition of red on blue or blue on red.

- Brown - is considered to be the boldest of all colors as well as the most exclusive and conclusive.

Colors manufactured by different commercial firms vary drastically in hardness, density, and coloration; it is desirable therefore that having started with a particular brand to continue with that brand and not intermix brands to ensure that distinctiveness and clarity are maintained.

A color ladder may be displayed graphically as follows:

COLOR	LEVEL (Qualitative)
BROWN	5
PURPLE	4
BLUE	3
RED	2
BLACK	1
GREEN	0

Another way to express the levels of the color ladder is by these definitions:

- BROWN - The ultimate in degree of trueness, not to be questioned. May also represent captured, compromised information or its equivalent.

- PURPLE - High in degree of reliability; may be used as a substitute or companion for brown where special conditions of clarity or distinction are vital to the problem. Primarily useful as a final ordered and oriented intermediate enjoying the same general stature as brown.

- BLUE - A relative base value having a significant bearing on the state of recovery.

- RED - A base of lesser value or no relativeness (completely arbitrary), a first step necessary in any endeavor.

- BLACK - To record or log information as it appears in its earliest or original form.

- GREEN - An envious color which is reserved completely for suspected garbles, projected or expected but unobserved values (not proven but highly suspected as being correct). Used to alter a meaning or information without obliterating the original (black) form.

Once a color scheme is established for a given problem, maintenance of color discipline is mandatory in order to achieve uninterrupted and unambiguous continuity. Discipline is also of great benefit to management in that it ensures that redistribution of analytic personnel can be effected with minimum disruption to the overall effort.

Postscript:

Colors:

Green - symbolized hope to the ancient Egyptians;

- in the Middle Ages was supposed to be good for the eyes;

- to the Mohammedan, a sacred color;

- in modern times has come to signify envy.

Purple - to the Tyrians and Romans, a purple robe or band of purple signified authority; became a symbol of majesty to the Romans.

Human Factors Corner

by [redacted]

☐ Some Advice to Users of **UN**friendly Systems (U)

☐ ...But What Do I Do With My Papers? (U)

I have received a number of responses to my article about "Unfriendly Systems" in the November 1981 issue of CRYPTOLOG. Several people have called to express their strong agreement with some of the points in the article, and to tell me some of their problems with the systems they are using. My impression is that, in some cases, the problems these users are reporting are of a serious and long-standing nature. It seems clear that, for several large classes of NSA computer users in key applications areas, problems with poorly-designed interactive software may be causing real and significant losses in personnel dollars and vital productivity.

For example, in one area which I won't name, users were at one time instructed by their supervisors NOT to make use of a major set of information support files designed specifically for their work, by an in-house computer support element in their own organization. Why? Because it was so difficult to get logged on, to frame a request, and to complete viewing responses without making an error. A user error caused the system to be locked up, preventing all users from getting at other things they needed until operations could be called to get the files closed and the user logged out. The procedure for getting into this system is still so complicated and unfriendly, and its response time is so slow once a user is into it, that many people avoid using it on line, and instead use hard-copy printouts. You may be wondering what terrible programming language this system could be written in to cause it to be so inadequate? The trouble lies not in the software system, but in the design philosophy of those who developed and implemented the user interface. The programming language is an excellent one, and provides rich and extensive facilities for composing convenient screen displays, and receiving user responses. No, we can't blame the computer or the programming language! Let's lay the blame where it belongs: on the designers of the user interface, whose philosophy goes something like this:

> "If those guys can't use our system, it's because they're too dumb! There's nothing wrong with OUR system! Anybody who comes around here complaining about OUR system is looking for a fight!"

What can you do about a situation like this? Those who have spoken to me about problems of this kind seem to have a defeated, fatalistic attitude. Some are quite bitter and angry. They have tried to tell their management about the problem, and the managers have tried to get something done about it, apparently with little success. I'd like to suggest an approach that may get you a little further: Put a notebook or lined pad near each terminal. Call it the "trouble log", "gripe log", or what have you. Tell everyone who uses the terminals to note every case of a problem with the system that he or she experiences. Note the name or initials of the user (so that you can find out more about the problem if need be), the date, time in hours and minutes, and as much detail as possible about the events that occurred. Note what was typed in or entered, what the response was, how long it took for the system to respond, and any other facts or events or times that show loss of user time due to deficiencies and unfriendliness in the system. Don't forget to note cases where the keyboard layout or design of commands needlessly leads users to make costly errors (for instance, when a user is very likely to destroy hours of work because the ERASE key is right next to the ENTER key, or a misleadingly-labeled command or field repeatedly leads users to make mistakes that

waste a lot of time over and over again, day after day, or an unhelpful response screen leaves users "up a tree" so they waste time trying to guess what went wrong).

After you have collected about a week to a month's worth of the trouble logs on all your terminals, study them and make a summary of what you have found. You can analyze the raw data in several useful ways. For instance, you will probably see certain recurrent problems that you suspected already, and which together account for the major proportion of your personnel dollars wasted at the terminal by users trying to use the system. You can write up a little paragraph on each, describing the problems that cause the wasted time, stating in man-hours and dollars (man-hours times your element's average hourly wage) the extent of the wasted resources, and recommending a change to improve the situation. If you can get your boss, and better yet, your bosses' boss, to do the same thing, and combine all the summaries into one memo to your machine support organization or whoever is likely to respond constructively, your memo will have even more impact. Keep up the trouble logs, keep on making monthly reports, and keep up the pressure. This course of action, if followed in a constructive way (not just angry griping), and backed up with good solid data on numbers of hours and dollars lost, should certainly get you a lot further toward a solution of the problems. It will also provide the machine-support management with a clearer idea of WHAT is wrong and some immediate ways in which they can improve the system.

You may well ask, what about the all-too-frequent cases where potential users of a facility or subsystem have simply given up, after many attempts, and now no longer use it at all? Or the case mentioned above, where a system is so punitive and unfriendly that supervisors have positively forbidden users to employ it, because it constitutes a menace to overall productivity? I suggest that you ask some of your potential users of such systems to keep a record of all the instances when they WOULD HAVE LIKED to use it, or to get at the information it contains. Try to get an estimate of the time and personnel dollars you would save, and the increase in quality of your product, if this aid were available and user-friendly.

These are just a few suggestions of ways you can "fight city hall", and improve matters for all of us, if you are a user of an unfriendly system.

...BUT WHAT DO I DO WITH MY PAPERS?

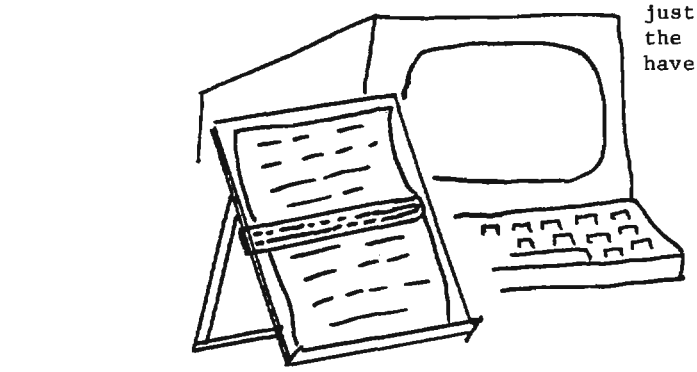
Reprinted from Human Factors Letter 4-80, published by the CISI Human Factors SIG.

Many of us who use CRT's may not be entirely happy with the response time or details of the user interface on the system. Even for those of us who are satisfied with these aspects of the system we use, however, there remains a stubborn problem that needs to be solved somehow. That is the matter of where to put papers, books, and worst of all, machine listings to which we must refer while we key things into the terminal. Various holders and racks are available, to sit on the desk or table and hold pages of copy, often with a horizontal bar or marker that can be moved or slid up and down to keep the place at a given line. These are adapted from aids in use by typists before CRTs came along. They might solve the problem, at least for page copy, if not for books or computer listings. In fact, I have rarely, if ever, seen anyone other than a typist or clerk using one of these devices in conjunction with CRT data entry, though they look as if they might be helpful. Elsewhere in this magazine, I have included some drawings of these gadgets, as advertised in a recent INMAC catalog of computer accessories.

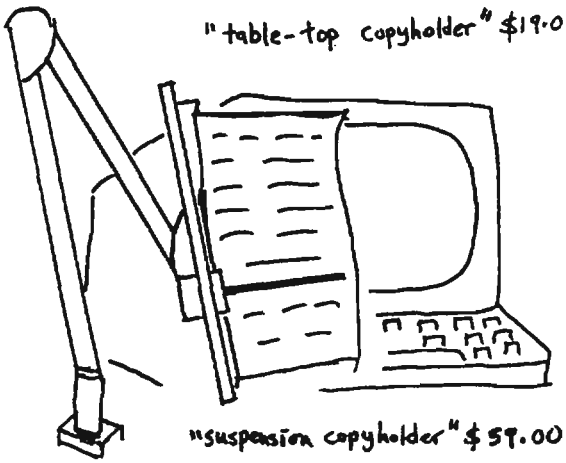
Users of CRTs are much more likely to prop folded bits of paper from which they must copy or extract information above the bank of keys on the keyboard, or against the terminal beneath the screen. Depending on the shape and size of the keyboard and the height of the screen above it, there is frequently some space to hold a small or folded sheet of paper there. Listings on size-12 paper, books, and thick documents must be laid open on the desk or table to the right or left (depending on which side you would prefer to have a crick in your neck that day). You crane your head to one side or the other, over your hands and arms which are busy typing at the keyboard, and reach across awkwardly to turn pages. If you are nearsighted, your troubles are exacerbated, especially with computer listings. These vast, cumbersome blocks of fanfold paper seem to extend for miles away from your eyes, and the line you want to see is all too often way up there at the very top. If you fold the listing over on itself, it is very likely to tear, or else to become dog-eared and dishevveled so that it never folds quite right thereafter. I have at times resorted to wrapping the listing around the edge of my table, pinching it against the table with my tummy, and squashing the top down so it sits in front of me just below the keyboard. Whatever else happens, sooner or later part or all of the fanfold falls onto the floor, unravelling itself to create an exasperating mess.

For users who aren't fortunate enough to have a terminal stand or desk wide enough or uncluttered enough to accommodate listings or papers beside the CRT, the lap or knees are the only solution. And, heaven help the user who needs to refer to several hardcopy documents at once while he is using the terminal! I have often seen users who must consult printed working aids and dictionaries trying to cope with five- and six-deep piles of books and documents in layers on their laps, the table, etc. while they paw back and forth from one to another trying to get the information they need to complete a transcript or report on the CRT.

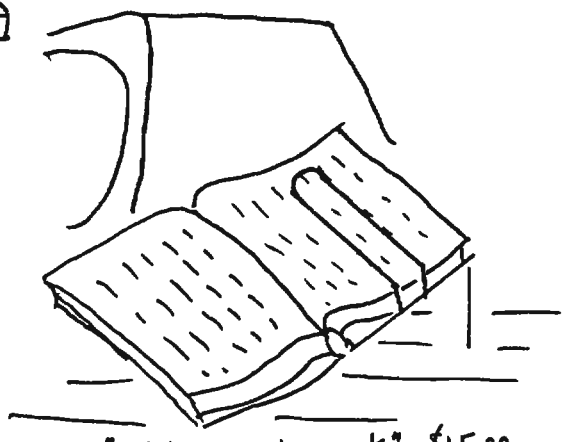
Perhaps, some day, a truly useful, comfortable, and efficient file structure will be available on line for many of the most frequently-consulted documents. There are now a few experimental systems that provide users with a "spatial" organization of different files, like the physical arrangement on the top of a very large desk or table. Such a system tries to help the user remember where he "put away" a given document when he discarded it temporarily to consult another, which documents or files he is working with, and where he is in each one. (A good example is the DATALAND system developed by Nicholas Negroponte and others at MIT.) Unfortunately, these systems aren't available to most of us just yet. In the meantime, until the state of the art catches up with this problem, we will have to live with it!



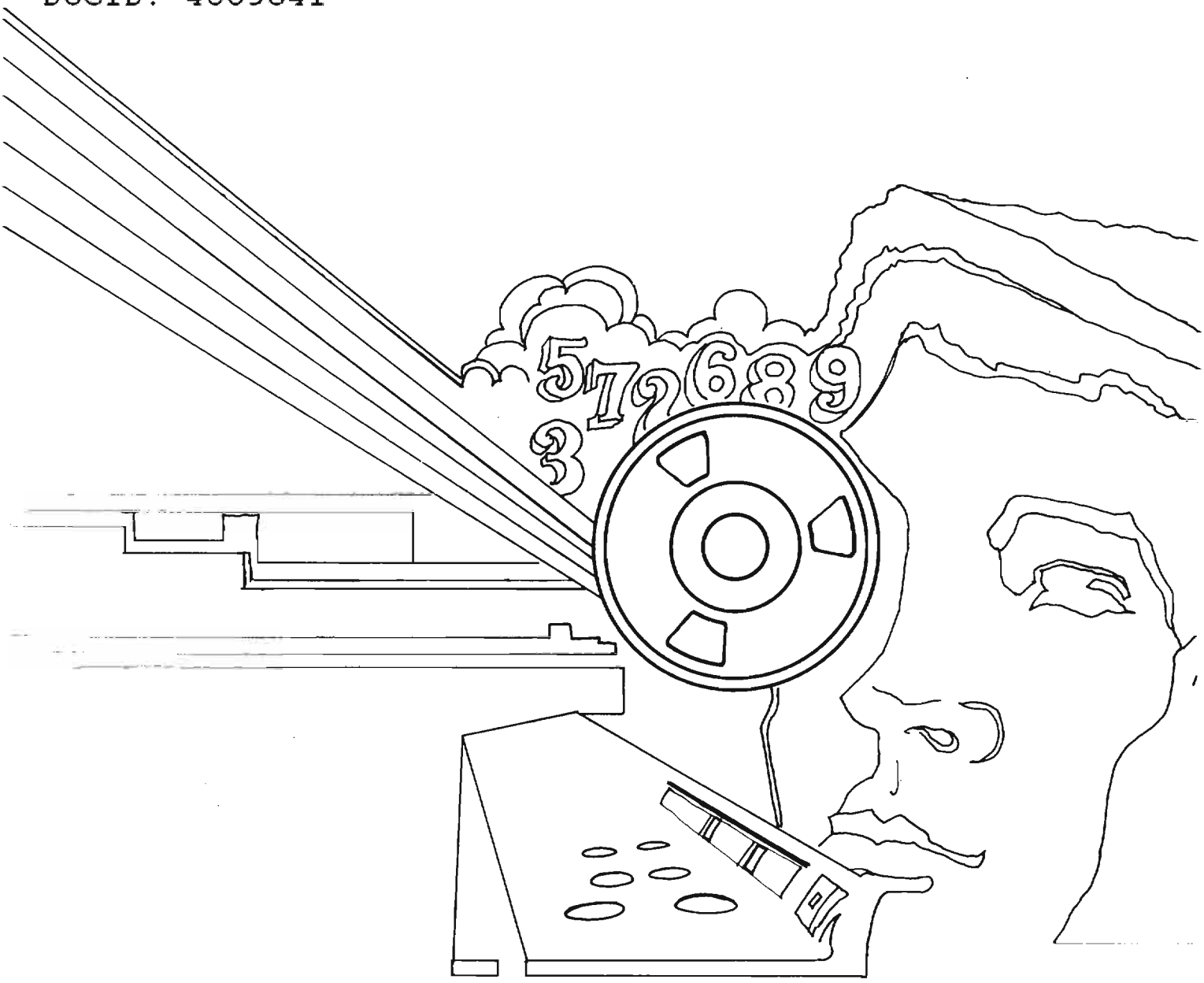
"table-top copyholder" $19.00



"suspension copyholder" $59.00



"printout reader rack" $15.00


5 7 2 6 8 9
3