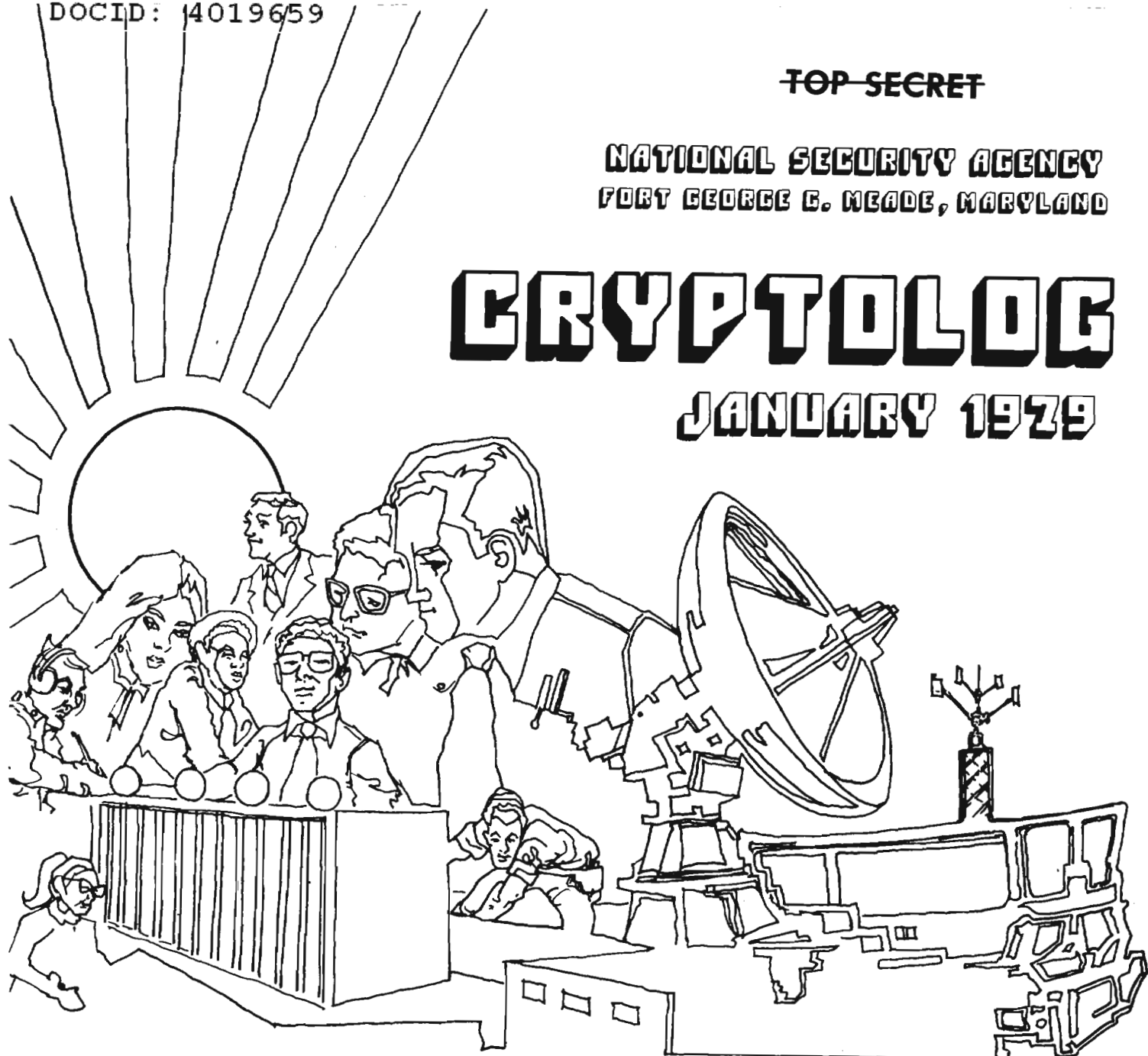


~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JANUARY 1979



SOLIS -- A VEHICLE IN SEARCH OF AN ENGINE.....	[REDACTED].....	1
HOW DO YOU TELL THESE TWO CLOWNS APART?.....	6
THE RETURN TO H.F.....	[REDACTED].....	7
SECOND SIGHTING.....	Sue Donym.....	12
JAPANESE TRANSLATION AT A.H.S.....	13
T-VISION: MEDIUM OF THE FUTURE.....	[REDACTED].....	17
REFLECTIONS AND RECOMMENDATIONS.....	Vera R. Filby.....	19
HUMAN FACTORS NEWSLETTER.....	[REDACTED].....	21
NSA-CROSTIC No. 21.....	David H. Williams.....	24
GOLDEN OLDIE: ON OPENING "STATISTICS".....	Marjorie Mountjoy.....	26
HENRY CEMENT & PHANTOMS OF OPERA(tions)	[REDACTED].....	27
CLASSIFICATION CORNER: IT'S PARTY TIME!.....	[REDACTED].....	28
PUBLISHER'S MESSAGE.....	29

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 2 JAN 2009~~

Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case # 54778

CRYPTOLOG

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

VOL. VI, NO. 1

JANUARY 1979

PUBLISHER

WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief.....Arthur J. Saleme (3957s)

Collection..... [redacted] (8955s)

Cryptanalysis..... [redacted] (4902s)

Cryptolinguistics..... [redacted] (5981s)

Language..... [redacted] (8161s)

Machine Support..... [redacted] III (5303s)

Mathematics..... [redacted] (8518s)

Special Research.....Vera R. Filby (7119s)

Traffic Analysis.....Don Taurone (3573s)

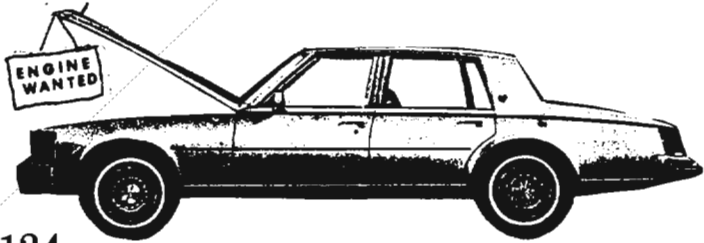
Production Manager.....Harry Goff (5236s)

P.L. 86-36

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

~~SECRET~~

SOLIS - A Vehicle in Search of an Engine



T124

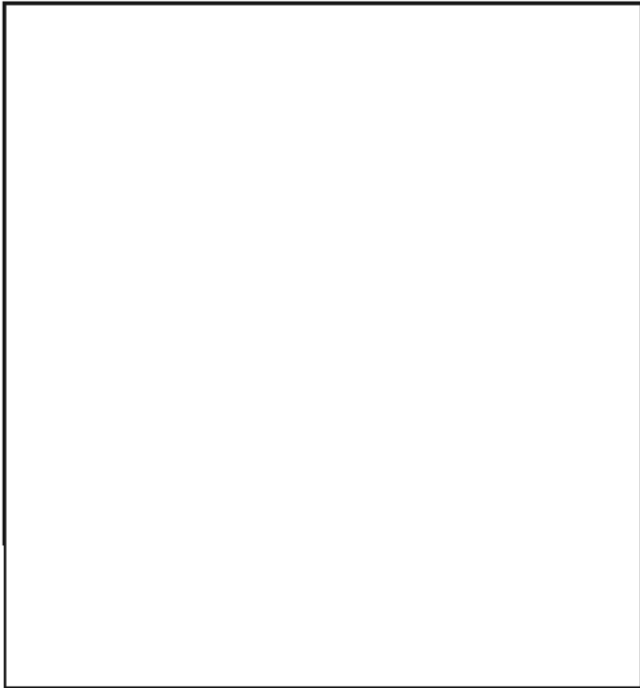
An Agency wit once remarked that "SOLIS has a Volkswagen engine in the body of a Cadillac." This statement evokes its share of nods and smiles. But why? What is it about this rather absurd little statement that made it humorous to SOLIS aficionados? The answer is that this metaphor had in it the germ of truth, and many hearers recognized this truth and could appreciate the way in which the wit expressed it.

The metaphor was first voiced in 1972. Today, nearly seven years later, it remains apropos.

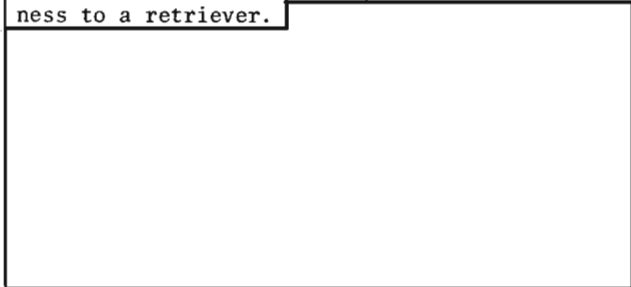
Let us, then, examine the system and the metaphor. What features of SOLIS remind one of the sensuous charms of a Cadillac body by Fisher? What is about the system that caused the wit to describe it as a grossly under-powered vehicle? To answer these questions it will be necessary to understand SOLIS -- its purpose, its organization, its operational philosophy -- and to take some measure of its performance as compared to the system developers' own loosely defined goals and expectations.

SOLIS -- the SIGINT On-Line Information System -- was born out of the experiences and frustrations of the HARVEST End-Product File Operation. For those of you who don't remember, asking a question of the HARVEST End-Product File could sometimes qualify as one of life's unique experiences, with the system's response ranging from "everything you never wanted to know about all subjects except the one you were really interested in" to "nothing at all." More often it was something between these extremes. But, since questions against the HARVEST File were batched and run only once or twice a week, you never knew what the response would be until you got a call to "Roll up your wheelbarrow" or to "Try again next week." Under these circumstances it is no wonder that SOLIS was developed as a viable alternative. It is only surprising that it took so long.

Before describing SOLIS in detail it would be well to impart some understanding of what is meant by the term "End-Product" or "SIGINT product." Storing and retrieving the product is, after all, what the HARVEST End-Product File (and its successor, STRONGBOX) and SOLIS were and are all about.



It was the sincere hope and belief of the system's first designer/planner that SOLIS could operate with a completely automatic indexing routine. After all, our experience with human indexers had not been a smashing success. It is difficult to get editing billets, it is difficult to fill them, and human editors are consistently inconsistent in their approach to editing. The SOLIS developer planned to avoid all these problems by developing a sure-fire, self-priming, automatic indexing routine. He would prepare indexing algorithms for the product serial, the date-time group, the "from" and "to" lines, the XXMM line, the content control code, and the other external data of potential usefulness to a retriever.



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

~~SECRET~~

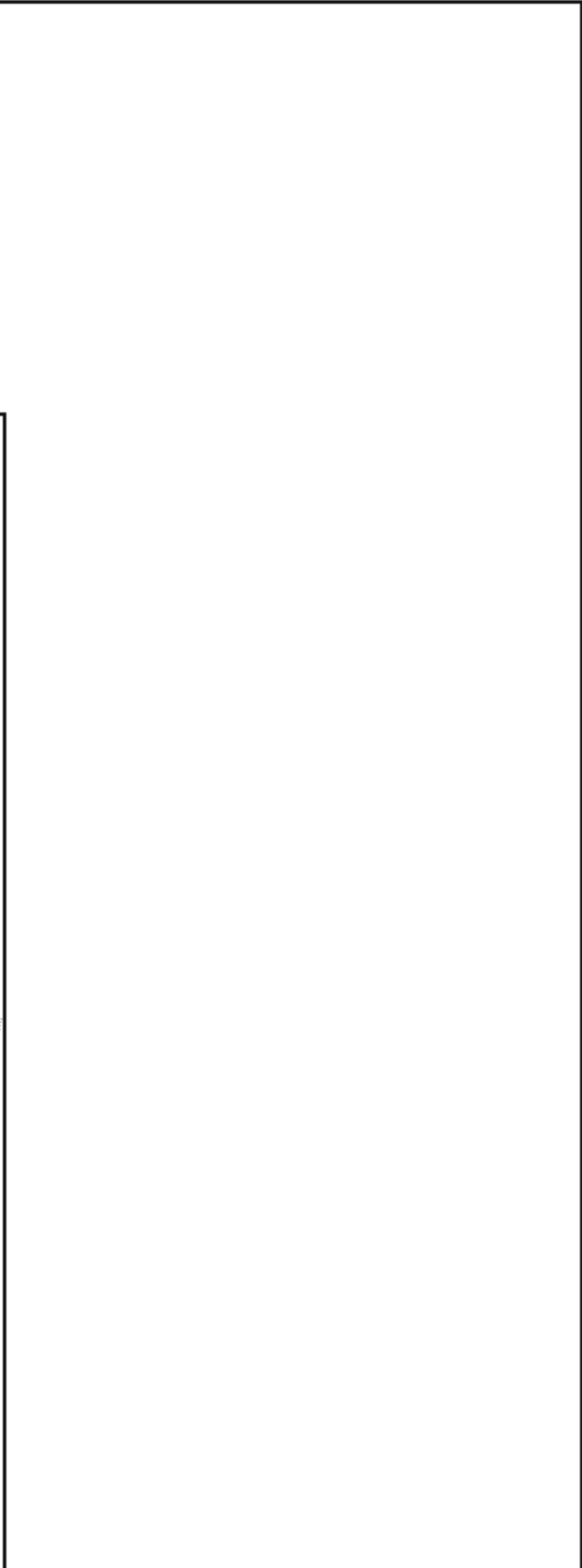
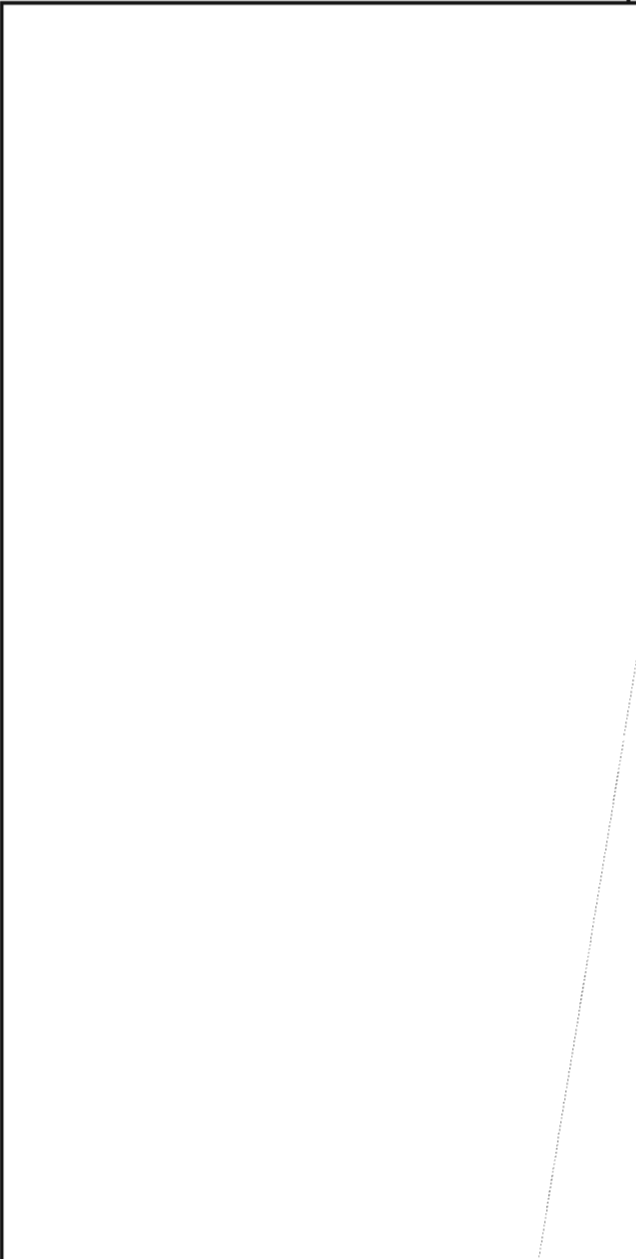
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~



SOLIS Programs and Procedures

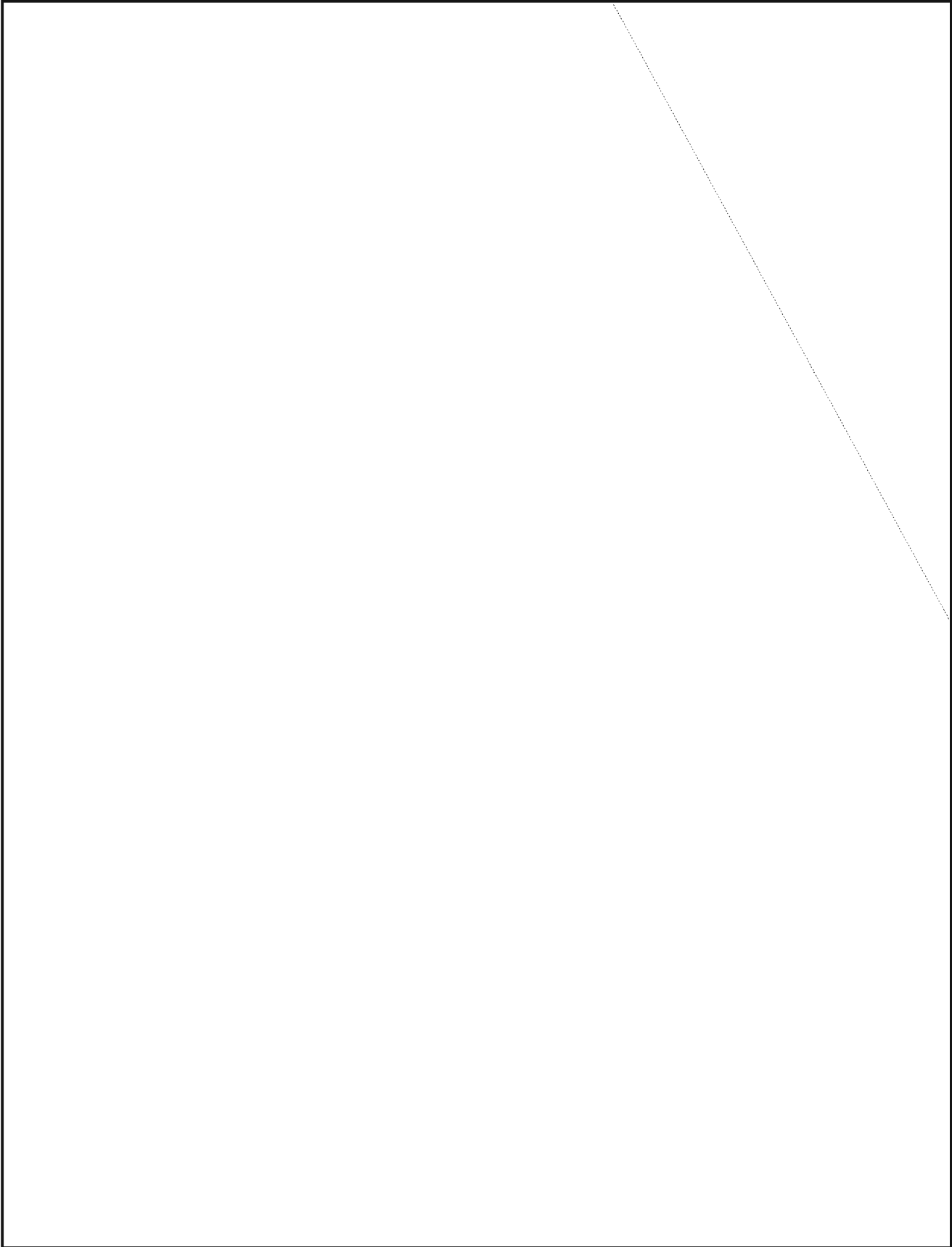
SOLIS today is a multitiered structure of programs and procedures that fit together into a harmonious whole.



~~SECRET~~

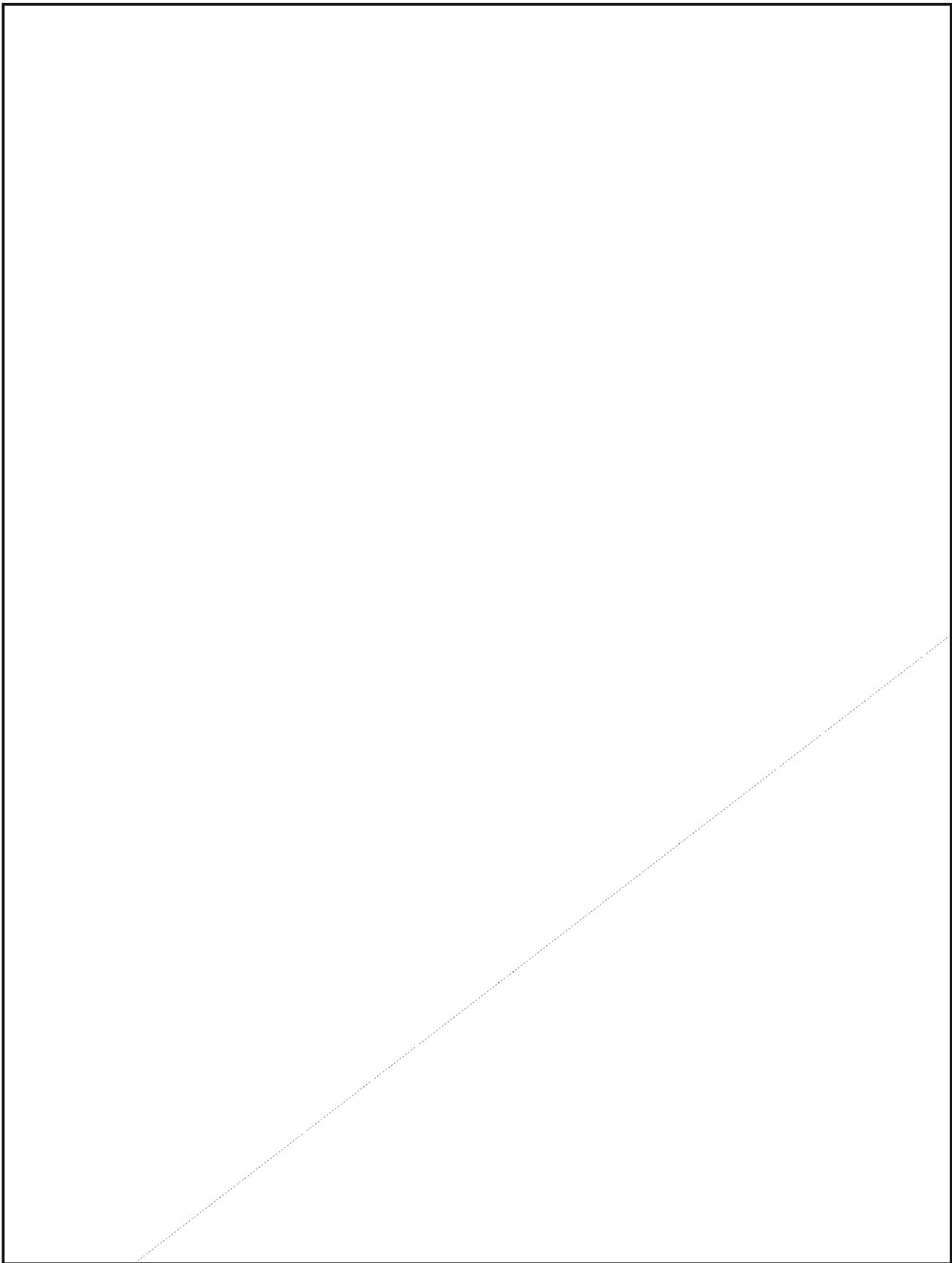
~~HANDLE VIA COMINT CHANNELS ONLY~~

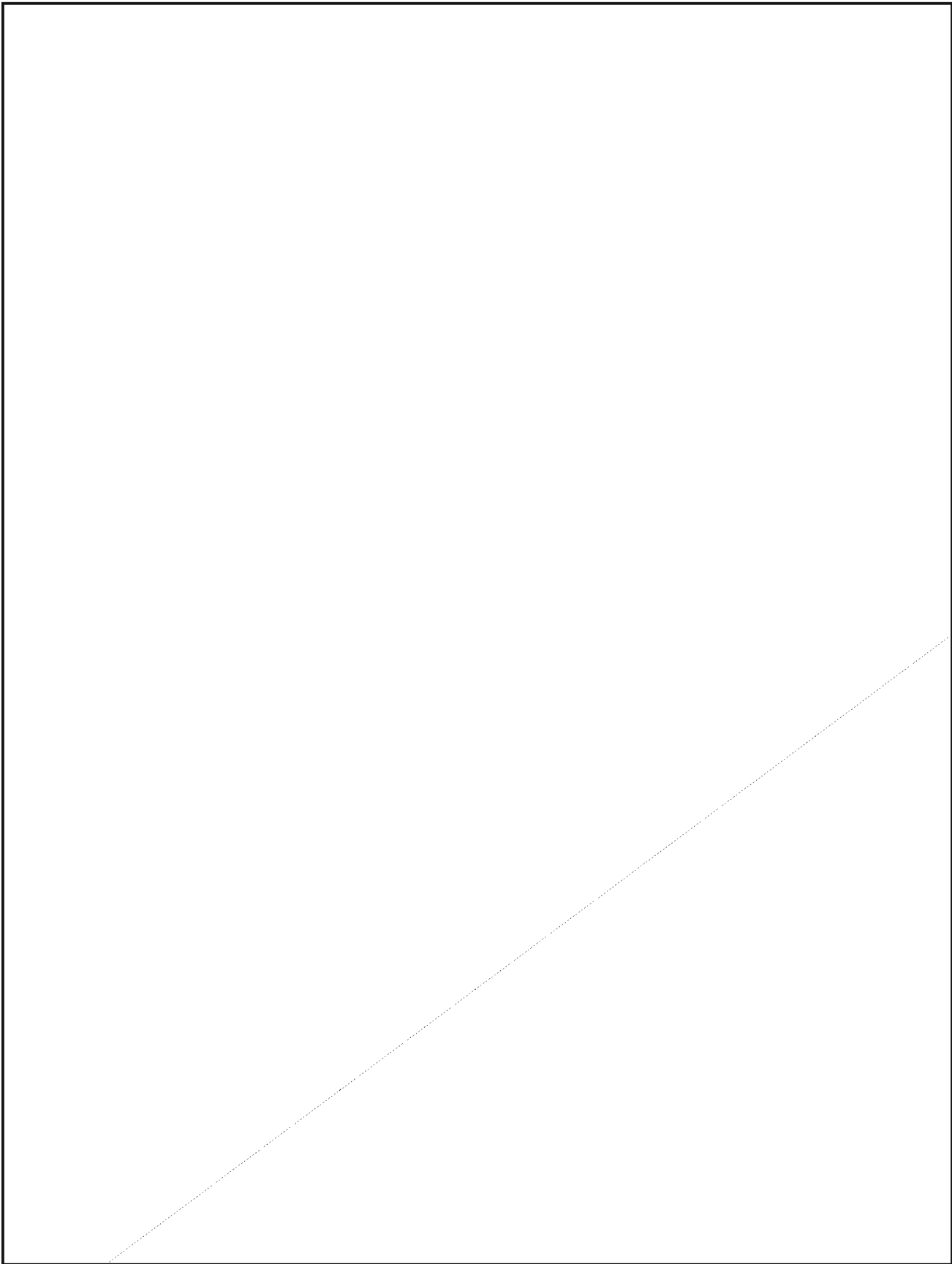
~~SECRET~~



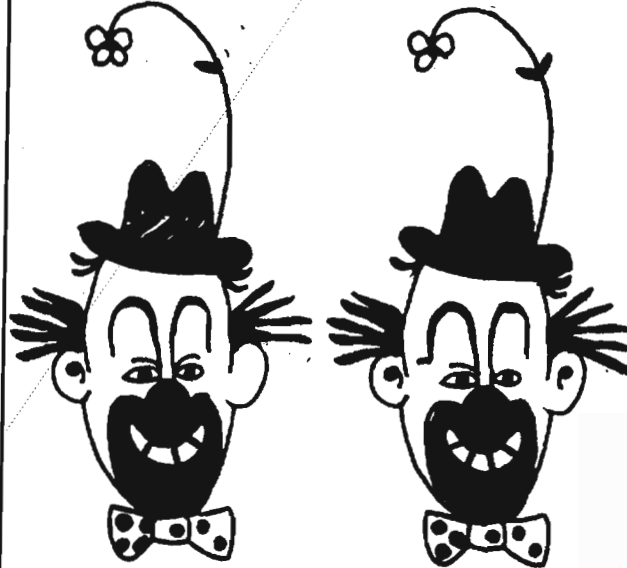
~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~





How do you tell these two clowns apart?



P.L. 86-36

There are ten differences between these two clowns. Can you find them?

Incidentally, some CRYPTOLOG readers are unaware that there are two Dave Williamses whose names have appeared frequently in CRYPTOLOG. One often gets blamed or praised for what the other does, so maybe we ought to call attention to the differences in the names and the contributions made by each Dave. Especially since one of them is going to become the Editor-in-Chief of CRYPTOLOG starting next month! (see page 29).

David H. Williams

David H. Williams has written an occasional item for CRYPTOLOG (most of his things appear in more prestigious Agency publications), but he is famous among CRYPTOLOG readers for his NSA-Crostics.

[redacted] (can you imagine what it must be like to be the one-hundred-and-eleventh person to bear the same name?) is our Machine Support Editor. He used to write more when he was the editor of the now defunct C-LINERS. For the past couple of years he has been helping CRYPTOLOG by persuading other people to submit articles on machine problems to the magazine.

Now, then, which Dave Williams is going to become CRYPTOLOG Editor in Chief starting with the February issue? It's the one with the H! The one with the [redacted] is going to continue as the Machine Support Editor. Maybe we can persuade [redacted] to write an article of his own as a test, just to see who gets the compliments! And, remember, if you like or dislike a definition in an NSA-crostic, don't tell [redacted] It'll be the wrong Dave!

(U)

(U)

SOLUTION TO NSA-CROSTIC No. 20
(CRYPTOLOG, December 1978),
By David H. Williams
(see next column)



Frances Blank, "It's Got to Get Out Today!", CRYPTOLOG, April 1977:

"One difficulty arose with electronic computers designed to translate from one language to another. The headline 'Mary suspended for youthful prank' was fed into a computer, translated into Russian, and then back into English. It came back as 'Mary hung for juvenile delinquency.'"

THE RETURN TO H.F.

P13

US. tactical forces intend to return to the use of HF radio for vital long-range communications, because of the vulnerability of satellites and cables. This conflicts with existing U.S. plans to give away the HF fixed service frequencies to the Third World at WARC 79*, on the assumption that the United States will rely on satellites from now on. A central issue is the military control of their own communication facilities, which is threatened by Congressional demands that the military *lease* satellite services, and no longer design and build military comsat systems. The technical issue is that satellite-era technology applied to HF makes HF cheaper and more reliable than satellites for certain kinds of traffic.

HF at AFCEA

Major General W. Hilsman, USA, in describing the "Electronic Battlefield of 1985" at AFCEA 1978 (1978 conference of the Armed Forces Communications and Electronics Association) included HF as a principal transoceanic medium to supplement cable and satellite for Army tactical needs. In response to a question about the future of HF in tactical communications, MGEN Hilsman -- who directs the tactical communications program -- said that a study 2 years ago had eliminated HF because satellite links were so much easier for the operator, but that he had completely "reopened the HF question." The field commanders like satellites, but realize they are highly vulnerable or may have long outages or even be canceled, so Hilsman is now training operators on SSB HF. Neil Birch, of C³I, followed this by saying that DoD is not "down on HF" and currently runs a "cemetery net" in NATO, and DoD is now looking at meteor-burst and adaptive-HF links. Birch had earlier spoken of HF as one of the triad (satellite, cable, HF) for a much-needed net of worldwide secure voice using 2.4 KB digital PARKHILL on analog voice encryption. Dr. N. McAllister, O/CNO, in speaking of Navy C³ for the future, noted that HF, employing new modular equipment afloat which will use digital filtering to extract signals from shipboard noise, is part of the "long term" Navy plan. He noted that there is keen competition between U.S. and EEC equipment, and said this was a primary area to achieve U.S.-NATO interoperations in equipment, communications, and operations. Cost is a key factor, and

*World Administrative Radio Conference, Geneva, 1979 -- see "Callsigns and WARC 79," by CRYPTOLOG, May 1978.

the Navy has recently had a FLTSAT canceled by Congress before it was launched because its costs were thought unfavorable compared to leased comsat services. Dr. Scheder of Rockwell, in reviewing future technology development for tactical communications, noted that HF could be greatly improved by using special IC digital processing to do frequency filtering of HF carriers to get rid of EMI on board ships, and to reject jammer energy. The Army expects to reduce the use of tactical voice traffic in the forward area -- even to the point of considering *no* voice -- because they cannot afford narrowband jamproof secure voice, but can afford jamproof and reliable data radio links which are necessary for fire control. Microprocessors and frequency-hopping radios with text displays and small keyboards will make this practicable as well as cheap -- and some of this equipment (e.g., RACAL MA 4230, 4231 auto morse sender/receiver/display) already exists.

The interest in HF and in data traffic instead of voice is not purely talk. The AFCEA exhibit, displaying the latest in military communications equipment in over 400 booths, was notable for displaying a variety of very modern HF equipment -- in over 20 booths -- including several major companies which have been making military satellites. It appeared that these manufacturers were alert and well informed about the U.S. military's interest in HF.

Navy HF Exercises

The U.S. Navy in the Mediterranean area shuts off its satellite from time to time to force the Navy operators to use their HF links. So far this has resulted in stress and traffic backlogs of a week or more, but the Navy is persisting in trying to resurrect HF operations. Presumably, foreign SIGINT finds the HF episodes interesting. The Navy MARS organization has built up a cadre of about 3500 to 4000 Navy amateurs who are given military frequencies to operate on, just to keep *some* HF capability. These MARS nets operate with SSB voice and NFKS printer to keep the operators trained and to keep the HF frequencies in use. Because of cochannel interference in the Mediterranean area, the operators much prefer the satellite links, but the Navy -- having had a recent FLTSAT program canceled -- cannot afford to become completely dependent on satellites. The MARS operators practically never use morse, but the NFKS printers -- also widely used on maritime circuits -- use filters as narrow as morse. These NFKS printers have replaced morse on most civil maritime mobile circuits, with much higher traffic capacity.

UNCLASSIFIED

LEASAT vs. HF

The LEASAT problem is also an important factor, for Congress feels that Defense monies can be saved by eliminating dedicated military satellites and requiring that the military departments lease satellite services from the commercial carriers. LTGEN Paschall, USAF, criticized this strongly, pointing out that the host country PTT would not allow a U.S. commercial-satellite link into Diego Garcia, while a military satellite would have been negotiated with the corresponding Defense Ministry. The tactical forces do not want to be dependent on foreign commercial satellites, and U.S. commercial satellites cannot downlink into foreign areas. Senior military officers declared forcefully at AFCEA that "lease vs. buy" was about equal in cost, but that the central issue was that the military had to control its *own* vital facilities, and had to use leased services as a backup for low-priority traffic. With telecommunications policy-making now shifted to NTIA in the Commerce Department, any new dedicated communications facilities used by DoD will be subject to policy control by NTIA, OMB, and OSTP, according to Executive Order 12046, and this gives further motivation for the U.S. military departments to reconstitute their HF capabilities, for U.S.-NATO tactical communications are not now subject to NTIA control by Executive Orders 11556 and 12046.

HF at ICC-78

However, a few weeks before the declarations of interest in HF radio at AFCEA, CAPT. J. E. Weatherford, USN (Ret.), who was a Navy frequency manager for 31 years, and a member of OTP until a few months ago engaged in WARC 79 preparations, declared at the International Conference on Communications (ICC-78) in Toronto that the United States expected to *give up* its fixed HF channels to the Third World at WARC 79 as part of its bargaining position. HF, he noted, would suit the southern-hemisphere countries very well. He also noted that the U.S. view was that northern-hemisphere countries could generally close down their HF fixed circuits because they had extensive satellite and cable circuits. For the United States, this would clearly be military HF frequencies, for there is not much nonmilitary U.S. fixed HF. The southern hemisphere, Weatherford said, was "starved for HF." He said "spectrum sharing" was crucial, and noted that elimination of local navids such as Shoran and Decca, etc., was planned. However, *expansion* of amateur radio frequency bands was under consideration because the amateur world was growing internationally and the Third World countries had found amateur radio very useful for disasters and emergencies because, among other things, northern-hemisphere "hams" have

given them enormous voluntary support in relaying and servicing messages, clearing all frequencies, and helping in every way. The South American countries in particular found the use of HF ham nets saved them the cost of emergency nets, and the long DX lets them work at uncluttered higher HF bands. Worldwide these are about a million hams, who operate all kinds of HF links by pooling a small portion of the HF spectrum, and knowledge of this high utility has impressed the governments in the LDCs (less developed countries) with the flexibility, independence, and low cost of HF communications.

Weatherford spoke authoritatively, outlining the OTP (now NTIA) position on the issues. He noted that the radio regulations were due for a major reworking at WARC 79, and that the non-government use of radio was going to dominate the U.S. position at WARC. The United States needs the support of the "nonaligned" nations to achieve its WARC 79 goals, and most of these countries are in the southern hemisphere. The position of the Third World LDCs is that they want to eliminate IFRB registration dates, and claim bands of spectrum for their own proposed future uses, which claim has been strongly resisted by the United States and the other Western industrial nations. At WARC 1974 the United States took exception to a provision of the treaty reducing U.S. shore station assignments. At WARC 1977 on satellite broadcasting, which culminated in the "one country -- one frequency" principle and in orbital slot limitations, the treaty is so unsatisfactory that President Carter will not send it to the Senate for approval. Now this political clash over the radio spectrum is to be resolved at WARC 79 by U.S. negotiations which will "trade off" HF frequency assignments which the U.S. tactical forces intend for major tactical backup. The U.S. position for WARC 79 was completed on 31 May 1978 and there was an SPM preparatory meeting on 23 October 1978 to consider the technical bases for WARC 79. The next GWARC will not occur until 1999, so WARC 79 will set the framework for radio usage and allocation for the rest of the century.

Technical Developments

There has been significant development in HF equipment, practices, and traffic growth over the last 15 years, while the U.S. military has virtually let their HF systems stand still or dwindle out of existence. Hence much U.S. military HF equipment and technique must be updated to modern low-cost digital electronics. Siemens predicts considerable growth in stations and traffic -- particularly data traffic -- for HF. Improved techniques such as SELCALL and channel pooling have reduced unscheduled message delays from hours to minutes over HF mobile links. Error rates as low as 10^{-5} and 10^{-6} on long links are regularly obtained by ARQ

UNCLASSIFIED

and error-central coding -- rivaling tele- phone lines. In the United States, HF can connect directly into the telephone nets. Where Al telegraphy of 30 years ago took a KHz of bandwidth to send 12 wpm (about 5 bps), modern NFSK and PSK systems regularly send at rates close to 1 bit/Hz, i.e. 100 baud NFSK in a 170 Hz SSB subchannel, or 3000 bps on a 20-tone 75-baud QPSK 3000 Hz SSB channel. This represents a 100- to 200-fold improvement in use of a single link, and the actual gain is even greater because of much greater accu- racy and full utilization of equipment. In addition to transmission improvements, better propagation forecasts, antennas, channel sounders, filters, etc., allow many more conventional carriers to operate concurrently at incomparably low cost. Siemens notes that a "marked increase has been achieved within the last few years in telegraph and data traf- fic, mostly over small radio stations which offer a maximum of economy." It is certain that any modern HF tactical radios developed for the U.S. military will very shortly be- come a demand item in world trade and tech- nology transfer, and will spread worldwide as comsats have.

In addition to conventional HF traffic, military spread spectrum systems have flourished to support strategic weapons sys- tems and other crucial links. HF spread spectrum transmitters can send chip-coded waveforms with bandwidths up to 20 percent of carrier, and frequency hoppers can span megacycles between pulses, with frequency stabilities of one Hz. The signals are jam- proof, undetectable, and a hot export item. WARC 79 will consider the introduction of spread spectrum signals into the nonmilitary and civil sectors.

The Policy Conflict

The fundamental conflict within the U.S. policy-making apparatus over HF was reasserted at EASCON 78 in September 1978, at an IEEE WARC meeting in October 1978, and in a *Washing- ton Post* editorial on 21 October 1978. At

EASCON 78 Captain Boslaugh, USN, of NAVELEX, outlined a plain for much increased U.S. Navy use of HF. The ELOS (Extended Line of Sight) HF ship-to-ship system will be the *primary* communication channel for fleet tactical commu- nications over ranges up to 300 miles, and will resist Soviet HFDF or jamming. Long-haul HF will be used to back up shore/ship satellite links. The Navy, having shut down HF stations to get money for satellite programs, is now putting them back into operation because it can- not get money for dedicated satellites. Cap- tain Boslaugh outlined a broad program of new equipment development for data and digital voice over HF. He also declared that no one could predict what would happen at WARC 79, but that frequency managers in the Pentagon feared the Navy might lose some of its resources, which could damage ELOS and other vital pro- grams. He also predicted that WARC would have the greatest effect on the long-haul HF commu- nications.

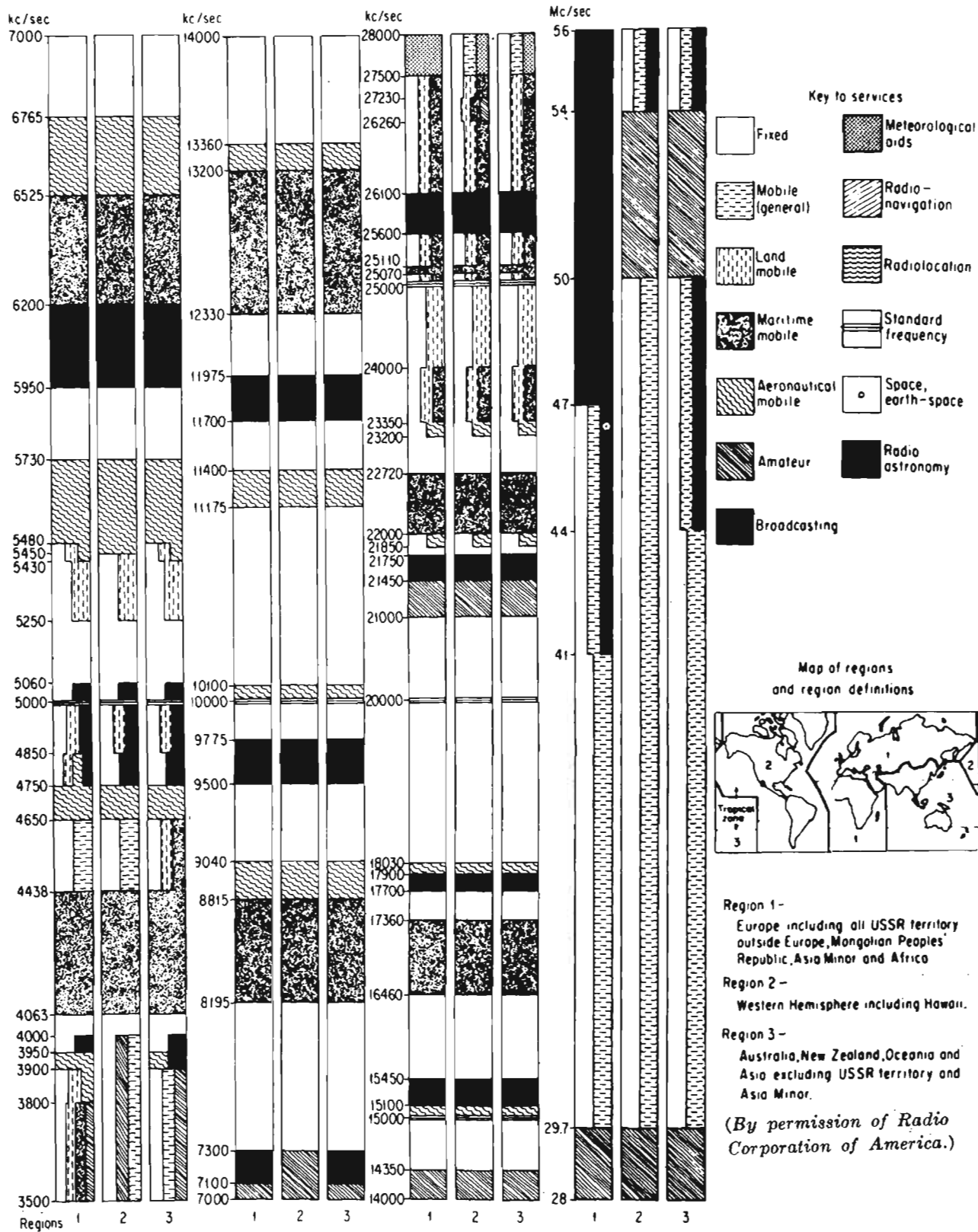
At an EASCON 78 seminar on C³I given by N. Birch of OSD, HF links were consistently shown as part of the triad of cable, satellite, and HF to give redundant C³ links.

At another EASCON 78 meeting on Frequency Management directly concerned with WARC 79, Leo Buss of NTIA and L. Petak of FCC both downplayed HF as a matter of secondary impor- tance at WARC, on the basis of responses to the NOIs. However, R. Shrum of the State De- partment, who had visited over 50 countries as part of the State Department's WARC prepara- tions, gave a completely opposite view at the same meeting. He declared that the three top- priority matters at WARC 79 for the LDCs were "HF, HF, and HF." His paper in the Con- ference Record stressed the same point and emphasized the political importance of HF al- locations to the LDCs. Shrum predicted that HF would be the "most contentious issue" at WARC 79.

The NTIA and FCC spokesmen claimed that the use of HF for fixed point to point circuits was going down because of satellites and

Present ITU band (kilohertz)	Existing service	Proposed ITU band (kilohertz)	Proposed new service
4438-4650	Fixed mobile except aeronautical mobile (R)	4438-4560	Maritime mobile.
5000-5250	Fixed	5200-5280	Do.
5250-5430	Fixed land mobile	5280-5300	Do.
6765-7000	Fixed	6950-7000	Amateur/amateur satellite.
7300-8185	do	8000-8185	Maritime mobile.
11975-12390	do	12130-12390	Do.
13360-14000	do	13360-13410	Radio astronomy.
13360-14000	do	13950-14000	Amateur.
14350-14990	do	14350-14400	Do.
15450-16460	do	16310-16460	Maritime mobile.
17360-17700	do	17360-17410	Do.
20010-2100	do	20010-20280	Do.
20010-21000	do	20950-21000	Amateur/amateur satellite.
22720-23200	do	22720-22855	Maritime mobile.

NOI-5 (WARC 79): "Portion of the spectrum proposed for reallocation to [Fixed Services]." (*Federal Register*, Vol. 42, No. 104, May 31, 1977, p. 27758.)



Radio-Frequency Allocation and Assignment (excerpted from *Communication System Engineering Handbook*, Donald H. Hamsher, Editor-in-Chief, McCraw-Hill Book Co.).

UNCLASSIFIED

cables, and hence were convinced that the United States could "trade off" the HF frequencies for LDC support on other issues. Other well-informed parties present, including a former NATO frequency manager, claimed the opposite, viz.: that HF use was increasing. The disagreement on this basic fact seems to stem from the data base used, and the NOI comments. The IFRB listings show that the use of fixed HF links for *public correspondence* has indeed gone down because of satellites. The U. S. users, e. g. AT&T, predicted a decline in fixed HF usage for public correspondence for the same reason. However, the IFRB data do not reflect what is actually happening in HF, for diplomatic and military and other *non-public* users are steadily encroaching on every unused HF channel and the ex-NATO frequency manager claimed that he combed the IFRB list for idle channels, assigning them ad hoc to meet the intense demand. Shrum said that many countries used HF for domestic links and never filed the usage with the ITU. The continuous sale of NFSK printer and other efficient modulation equipment suggests that the users are passing more and more traffic, while IFRB only registers the *proposed* usage, not the actual traffic intensity. The result is that U.S. WARC policy is being formulated from an unclassified data base which does not show the non-public usage, domestic usage in other countries, unregistered usage, the effects of new equipment, or the projected usage by U.S. and NATO military communications.

The NTIA view of HF as a bargaining chip, based on "declining usage," was repeated on 13 October 1978 by Buss at an IEEE meeting on WARC. A *Washington Post* op-ed column on 21 October 1978 by G. Kroloff, formerly of the Senate Foreign Relations Committee, also advocated giving up HF bands to the Third World, while a speech by Senator H. Schmidt (R-N.M.) chided U.S. WARC preparations for being left to technicians who were not protecting U.S. policy and economic interests (*Satellite Communications*, September 1978).

The final U.S. position must be completed and sent to Geneva by the end of January 1979 and the most basic facts and decisions about HF and its importance to the United States are still unsettled. The military users view HF as integral, to tie together many nets and to back up and reconstruct nets of all kinds in case of outages or war damage to other circuits, while NTIA and FCC see nonmilitary policy issues about broadcasting, radio astronomy, satellite sensors, and other non-HF matters as more important.

The Communications Act of 1978

The difference in point of view between U.S. military communicators who want dedicated facilities which they can control, and the NTIA-FCC WARC team which apparently wants HF

frequencies to dispose of as a bargaining chip, will be intensified if the newly issued *Communication Act of 1978, H.R. 13015* is enacted before WARC 79 as expected. This Bill, drafted by former TV newsman Van Deerlin, would transfer most of the FCC functions and all of the NTIA functions and people to an independent agency, the National Telecommunications Agency (NTA). NTA will do policy-making for *all* U.S. telecommunications, including DoD. It will control all frequency allocations for government and nongovernment users, and will resolve all interagency telecommunication differences. NTA will prepare and manage U.S. participation in international telecommunications conferences, and will develop plans, policies, and programs for government telecommunications. NTA will serve as the principal advisor to the President on telecommunications issues and policies and may absorb the functions of any government agency which relate primarily to development or implementation of telecommunications policy (including privacy). In particular, NTA will coordinate development and operations of emergency telecommunications systems, and will participate in the development and operation of national-security telecommunications systems. Unlike the 1934 Act, this new Bill, H.R. 13015, has *no* war-powers provisions corresponding to 47 USC 606, so that the military departments, or the President, cannot take over or control radio or civil telecommunications in a war emergency or a war. This will have the effect of limiting the military services to the frequencies and facilities they have at the start of a war, or which they are able to lease under NTA guidance, and this could affect the renewed U.S.-NATO commitment to HF -- possibly by forcing much greater joint use and sharing of U.S.-NATO military frequencies under agreements that lie outside of NTA's scope.

Prospectus for HF

Despite the internal U.S. situation, the prospects for growth of HF traffic for military, commercial, diplomatic, maritime, aircraft, weather, news-agency, security-forces, emergency nets, etc., and even for scientific data and economic aid, seem irresistible. The improvements in radio and processor technology, and low-cost displays, will bring the cost of equipment down markedly, and greatly improve traffic handling for messages and data. Many different kinds of traffic will flourish, including voice, narrow-voice, data, fax, TTY, morse, slow-scan video and graphics, telemetry, telecommand, etc. Improvements in weapon guidance can assure destruction of U.S. and NATO fixed trunks and switches, and most satellites cannot withstand EW. Hence, existing communication nets must be discounted for war fighting. On the other hand, the resistance of HF nets to EW and to nuclear bursts

UNCLASSIFIED

UNCLASSIFIED

and blackouts is better understood than 15 years ago. With microprocessors and memories to interface between the users and the tricky HF circuits, easy and reliable communication to any point can become a commonplace. Traffic demand will encourage brevity codes, and data compressors, and channel pooling. In 1963, HF traffic was estimated by ITU at several million wpm. NAE (National Academy of Engineering) in 1972 estimated that a 19-fold growth in HF channel usage was possible by better technique. Current state-of-the-art

technology could give data traffic over more than one million different links simultaneously. at total traffic rates above 500 billion words per day -- about 10⁴ greater than the WW II Army ACAN net.

The demand, technology, mass market, and allocation-usage arrangements are all coinciding and WARC 79 will be a major factor in determining how fast this "modern HF" traffic develops.

(U)

SECOND SIGHTING

By



Some time ago -- well, actually, a long time ago -- we traffic analysts had a word in our vocabulary that we enjoyed using. It was a good word, and we enjoyed using it because it expressed exactly what was meant. Other people could use the word too -- it wasn't jargon at all.

Everything went well for the word for a number of years. Writers used it, and readers understood it. It wasn't controversial, either. After a while, though, a group of newcomers began writing reports about traffic analysis, and they used *another* word to express the same concept.

We commented that their word, a perfectly good word itself, was not exactly correct when used in a TA context. They countered that *our* word was a no-good word because it wasn't in any dictionaries and their word was a good word because it *was* in dictionaries. They were correct when they said our word wasn't in dictionaries, but we insisted our word really was a good word, because it was a compound word and we had followed rules for forming compound words. Besides, the two words (our word and their word) are pronounced differently -- that means they couldn't possibly be the *same* word. Not only that, but there are lots of NSA words that aren't in any dictionaries.

Neither side gave in. We used our word and they used theirs. Whenever we could, as editors or prepublication report reviewers, we changed their word to ours. Their feelings were ruffled and we had many arguments, often quite loud ones.

The other-word people began to spread like fungus throughout the building, and some of them were in positions to change *our* word to *theirs*. Now *our* feelings were ruffled and, again, we had many arguments, often quite loud ones. One argument was so loud that a decision had to be made about which word to use. A disinterested third party at NSA, caught unwillingly in the argument, asked a disin-

terested fourth party on a high-level staff to make the decision. He did! He, or some of his staff or a committee, decided that a *third* word would be used. Traffic analysts here, on ships at sea, in the air, on foreign soil, and everywhere gradually began to use the third word. We weren't too happy with it because it looked like a misspelling of that *other* word, but all went reasonably well. At least we weren't having those arguments any more. All continued to go reasonably well until that third party, the very one who asked for the dispute to be settled, took some papers to a *very* high-level staff to be signed by a *very* high-level person. A member of the very high-level staff read the papers, saw the third word, marked it out, and replaced it with (gasp!) *that other word!*

Here we are again. That other word is now used by writers at very high levels. Traffic analysts use the third word.

However, we are beginning to have some hope for our word. We saw it in a dictionary¹ three or four years ago -- first sighting! Today we saw it in a book² ". . . intended to familiarize a wide audience with telegraph and data communication over short-wave links" -- second sighting!

We are looking forward to the third sighting. Who knows, we might get our word³ back again.

¹Webster's New World Dictionary of the American Language, Second edition, 1972.

²Telegraph and Data Transmission over Shortwave Radio Links," Lothar Wiesner, Siemens AG, Berlin and Munich; Heyden & Son, Ltd., London.

³Our word (gaining fast): ("co-locate"; their word (bool hiss): ("co-locate"; third word (new but is it improved?): "co-locate".

(U)

UNCLASSIFIED

~~TOP SECRET UMBRA~~

PAGES FROM THE PAST

W.W.II JAPANESE TRANSLATION

Japanese Diplomatic Section,
U.S. Army Signal Corps Signal Service Unit,
Arlington Hall Station, 1945

AT ARLINGTON HALL STATION

The following are excerpts (Chapter IX, "Conclusion," pp. 100-104, and Appendix B, pp. v-viii, of "History of the Signal Security Agency, Volume Four: The Language Branch," Army Security Agency, Washington, D. C., 15 September 1946 (TS). A copy of the original document (with file number L-441) is available in T1213, Room 2N090, x5759s.)

Ed.

Translation is only one step in the long process of rendering intercepted enemy communications intelligible to those who plan Allied strategy, but it is the ultimate step, for only expert, careful translation can reveal the import of enemy communications and transform them into vital information."

This statement was the prize-winning entry in a contest participated in by Language Branch personnel in the summer of 1944, and it expresses simply but eloquently the attitude of the translators toward their mission. Deeply conscious of the responsibility which was theirs -- and, indeed, it was a great responsibility, since upon their knowledge and ability depended the final exploitation of the product of thousands of other persons engaged in the interception and cryptanalysis of the most secret communications of the Japanese Empire -- almost to a man they fell to with enthusiasm and devotion, determined to get the most out of the material which was provided.

A review of production figures during the war (that is, from Pearl Harbor through August 1945) reveals that the Language Branch scanned considerably more than 1,100,000 decoded messages in all categories, out of which approximately 415,000 were forwarded to the Military Intelligence Service in the form of transla-

tions. This was a record far beyond what could have been anticipated or even imagined at the outset, when the force of Japanese translators consisted of only nine persons. It is believed to be an achievement of which all who participated can be proud.

In bringing this history to a conclusion, the following further observations have been appended with the thought that they might be helpful in determining procedures should similar situations have to be dealt with in the future.

Regardless of the language used, the linguistic aspects of any problem involving the exploitation of codes and ciphers are necessarily associated in a very intimate way with the cryptanalytic aspects. As a matter of fact, close coordination between translation and cryptanalysis is regarded to be of such importance that under normal circumstances the two functions are integrated within a single administrative organization.

But, as has been described in considerable detail in preceding chapters, during the war Japanese translation at Arlington Hall became such an extensive and diversified operation, presenting training and technical problems of such complex and unusual character, that it soon became necessary to place its administration on an independent, self-contained basis.

As it worked out, not only was the handling of training and translation problems greatly facilitated thereby, but the cryptanalysts, who depended upon the translators for assistance, also gained by this separation. What actually happened was that translators were attached to cryptanalytic units on temporary loan when and as needed. Meanwhile, however, through their administrative connection with the Language

~~TOP SECRET UMBRA~~

Branch, they were kept in direct touch with the developments in the knowledge of the Japanese language, so that the quality of their aid to the cryptanalysts was constantly improved. Also, under this arrangement, it was possible to exercise much more selectivity in the allocation of jobs than would have been possible otherwise, and to place individuals on specific assignments, whether straight translation, code reconstruction, scanning, research, or auditing overlaps, in accordance with their ability to handle the specific assignment.

If there was any one special feature of Language Branch operations which contributed more than others to the success of the entire venture, it was the principle of flexibility, under which personnel who developed most along certain lines could be easily shifted from problem to problem where these skills might be best utilized. Thus, some individuals had a natural flair for straight translation, others for scanning, or for code reconstruction, or for cryptanalysis. In addition, translators had different backgrounds of experience and knowledge which made them individually valuable in specialized subject categories, such as Diplomatic, Commercial, Scientific, Order of Battle, and Shipping. These individual aptitudes did not usually show up at once when the translators came into operations but manifested themselves gradually as the translators gained further experience, so that it took time for each one to settle into the niche where he could do his best work.

If, by virtue of a different type of organization, the translators had to be parceled out to various crypto-translation units as they came into operations, there to be assigned on a permanent basis, obviously this flexibility, this opportunity for watching them and eventually fitting them into the right occupations would largely have been lost, with consequent detriment to the overall production effort. As it was, when urgent code reconstruction jobs came along, to pick one example, personnel experienced in that type of work were given the responsibility; and the same allocation of workers to jobs in which they were apt took place all along the line.

It is desired to make one more reference to the work of the Special Projects Section of the Language Branch. Although in the beginning there was no intention of going into the compilation and publication of dictionaries and other word studies on any elaborate scale, but merely to record and make available in useful and organized form such lexicographical information as emerged during the course of operations, the need for expediting the production of translations by anticipating the linguistic problems of the translators naturally caused the projects to expand far beyond what was originally contemplated. How the work was carried on, what sources of information were utilized, and the nature of the published

results have been described in Chapter V of this history. What it is desired to emphasize here is that during the war this Section developed into what was probably the most scholarly, the most efficient, and the most valuable Japanese language research body in the United States.

The contribution of this Special Projects Section to the solution of every department of the Japanese problem as encountered by the Signal Security Agency during the war effort cannot be overestimated. What was actually done was to provide ever finer and ever sharper tools to the end that the time and labor of those engaged in direct production could be more effectually utilized. But -- and this is a point which should not be lightly overlooked -- the beneficial results of this Section's work may be even more far-reaching in the future if the work is permitted to go on and, furthermore, if free dissemination of the products is allowed to all who can profitably use them. Large segments of the findings of the Special Projects Section, although available in the files, have not yet been published, and much more can be accomplished if the Section is allowed to continue its endeavors. It is greatly to be hoped that the fine beginning which has been made in this extremely significant field of Japanese lexicography will not be allowed to lapse, but that arrangements will be made by which there may continue to be made available new knowledge on this complex subject.

APPENDIX

Language Branch

Chronological Table of Principal Developments

<u>Item</u>	<u>Date</u>	
1	<u>1930</u> May	First Japanese translator employed, Mr. John B. Hurt. Activities mainly cryptanalytic research
22	<u>1935</u> March	First formal Japanese translation published
33	<u>1937</u> February	First "Red" translation (machine cipher system)
44	December	One-thousandth translation
55	<u>1938</u> March	Second translator employed, Mr. Paul Cate
66	<u>1939</u> September	First "Purple" translation (machine cipher system)

~~TOP SECRET UMBRA~~

- | | | | | | |
|----|-------------------------|--|----|------------------------|---|
| 7 | <u>1940</u>
January | Third translator employed, Mr. Hugh S. Erskine (later Lt. Col. and Chief of Translation Section, Central Bureau, USAFFE) | 28 | August | Auditing Unit set up to assist cryptanalysts (JEM) |
| 8 | October | Fourth translator assigned to active duty, Lt. Verner C. Aurell (later Lt. Col. and Chief, Language Branch) | 29 | August | Reconstruction begun on Diplomatic code JBB (old JCV) |
| 9 | December | Translations appearing in eight Japanese Diplomatic systems ("Red," "Purple," CA, YO, LA, J-17, PA, P-1) | 30 | August | First JBB translation published (see item 29) |
| 10 | <u>1941</u>
June | First J-18 translation published | 31 | September | B Branch reorganized. B-1 functions limited to Japanese language activities |
| 11 | September | First J-19 translation published (JAE) | 32 | September | B-1 organized into four sections as follows: B-1-R (Army Translation), Capt. Overton, OIC; B-1-D (Diplomatic Translation, Lt. Bacon, OIC; B-1-M (Military Attache Translation), Mr. Millard, CIC; B-1-JS (Japanese School), Mr. Buchanan, CIC |
| 12 | September | First J-22 translation published (JAI) | 33 | September | First ASTP class started at Georgetown University |
| 13 | December | Pearl Harbor. Japanese Translation Unit consisted of nine persons | 34 | September | Auditing Unit set up to assist cryptanalysts (JEK) |
| 14 | <u>1942</u>
May | First two translators to overseas duty (Erskine, Mahrt) | 35 | September | Translator team plan adopted in B-1-R |
| 15 | June | Reconstruction begun on Military Attache Code (JAS) | 36 | October | Captured Army Communications Code Book translated (JBT, later designated JER) |
| 16 | August | Translators organized as subsection B-1-J under Capt. Aurell | 37 | October | Reconstruction begun on Diplomatic Code JBA |
| 17 | August | First JAS translation published (see item 15) | 38 | November | Reconstruction begun on Japanese Army ship name and place name auxiliary codes |
| 18 | September | Japanese Language School established (30 enlisted students) | 39 | November | Reconstruction begun on Army Administrative Code Book No. 4 (see also item 27) |
| 19 | November | Aurell made OIC, B-1; Overton made OIC, B-1-J (see item 16) | 40 | November | First JBA translation published (see item 37) |
| 20 | December | First five graduates from J. School entered operations, bringing total translator staff to 28, including three instructors | 41 | November | Reconstruction begun on Diplomatic Code JBC |
| 21 | <u>1943</u>
February | First translator assigned to Japanese Army systems under cryptanalytic study | 42 | December | First translation published in Army Administrative Code Book No. 4 (see item 39) |
| 22 | April | Japanese Army Translation Subsection (B-1-JR) organized | 43 | December | Reconstruction begun on Army Air Code Book No. 3 (JES) |
| 23 | April | Reconstruction begun on Water Transport Code Book No. 1 (JCN) | 44 | December | Total translator staff (including nine instructors) -- 121 |
| 24 | June | First JCN translation published (see item 23) | 45 | <u>1944</u>
January | 43 enlisted translators commissioned 2nd Lieutenants. |
| 25 | June | Code Instruction Translation Unit set up in B-1-JR | 46 | January | Reconstruction begun on Military Attache Code No. 3 (JAS, see item 15) |
| 26 | June | Routing and Logging Unit set up in B-1-JR | 47 | January | Captured auxiliary code books translated (see item 38) |
| 27 | August | Reconstruction begun on Army Administrative Code Book No. 3 (JEM) | 48 | January | Captured Army Administrative Code Book No. 4 translated (see item 39) |
| | | | 49 | February | First JBC translation published (see item 41) |
| | | | 50 | February | Vint Hill Nisei translation set up |
| | | | 51 | February | Translations begun on Army Administrative systems based |

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

- 52 February Scanning Unit established for Army Administrative decodes
- 53 February Reconstruction begun on Army Communications Code Book No. 2 (see item 36)
- 54 March B-1-R Liaison Unit set up for handling queries
- 55 March B-1-R Research Unit set up for stereotypes and isologs
- 56 March B-1-R translator teams specialize (see item 35)
- 57 April Reconstruction begun on Diplomatic system JBD
- 58 May 15 enlisted translators commissioned 2nd Lieutenants
- 59 May B-1-SP Special Projects subsection organized under Dr. Nelson
- 60 June First JBD translation published (see item 57)
- 61 June B-1 celebrates achievements to date
- 62 July Translations begun in Army Air system (see item 43)
- 63 July Translator unit attached to Traffic Analysis, Section B-IV
- 64 August First JBL translation published (transposition)
- 65 August Reconstruction begun on Army "BULBUL" low-level code
- 66 August B-1 becomes Language Branch under Intelligence Division
- 67 August B-1-V becomes section under Language Branch (see item 50)
- 68 September Captured Communications Code Book No. 2 translated (see item 53)
- 69 September Captured Army-Navy Liaison Code Book No. 4 translated (JEH)
- 70 September First JBN translation translated (Commercial system)
- 71 September Chief B-1 leaves for TD, SWPA (2 months)
- 72 October Captured JKY Army code translated by B-1-V
- 73 October Reconstruction begun on Army Water Transport Code Book No. 2 (see also item 23)
- 74 November Reconstruction begun on Diplomatic Code JAM
- 75 November First JKY translations published (see item 72)
- 76 December First JAT translation published (Military Attache system)
- 77 December Language Branch personnel at end of 1944:

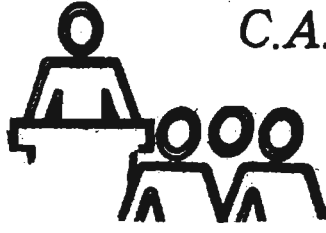
Translators	254
Trainees	170
Administrative and clerical	92
Vint Hill	63
<i>Total</i>	<u>579</u>

- 1945
- 78 January First JAM translation published (see item 74)
 - 79 January B-1-C Commercial Translation Section organized under Lt. Bohannon
 - 80 February Reconstruction begun on Army Administrative Code Book No. 5 (see also item 39)
 - 81 March Reconstruction begun on Army Air Code Book No. 4 (see also item 43)
 - 82 March Translations begun from item 81 (above)
 - 83 April Translations begun from item 80 (above)
 - 84 April First JHC translation published (UNEIKAI)
 - 85 May Plain text scanning unit set up in B-1-C
 - 86 June 100,000th Army Administrative systems translation published
 - 87 June Captured JEC Army Air Code Book translated
 - 88 June Captured Army Administrative Code Book No. 5 translated (see item 80)
 - 89 July Captured Army Communications Code Book No. 3 translated (see also item 68)
 - 90 July Captured Army Air Code Book No. 4 translated (see item 81)

The copy of "History of the Signal Security Agency" from which the preceding excerpts were taken was provided by the NSA Cryptologic History and Publications Staff, DA.

(TS)

1979 C.A. SEMINAR



It may not be too late for you to sign up for the fourth annual seminar, "Cryptanalysis: Contemporary Issues," which the CA Division of the National Cryptologic School will present at Fort Meade from 30 January through 1 February. Sixteen speakers will cover various topics of interest to cripplies. Although professional cryptanalysts get first pick, the seminar (CA-305) is open to all cleared and indoctrinated people. Sign up through your training coordinator.

For additional information, call: P.L. 86-36

CA Division, NCS, E42, 8025s. (U)

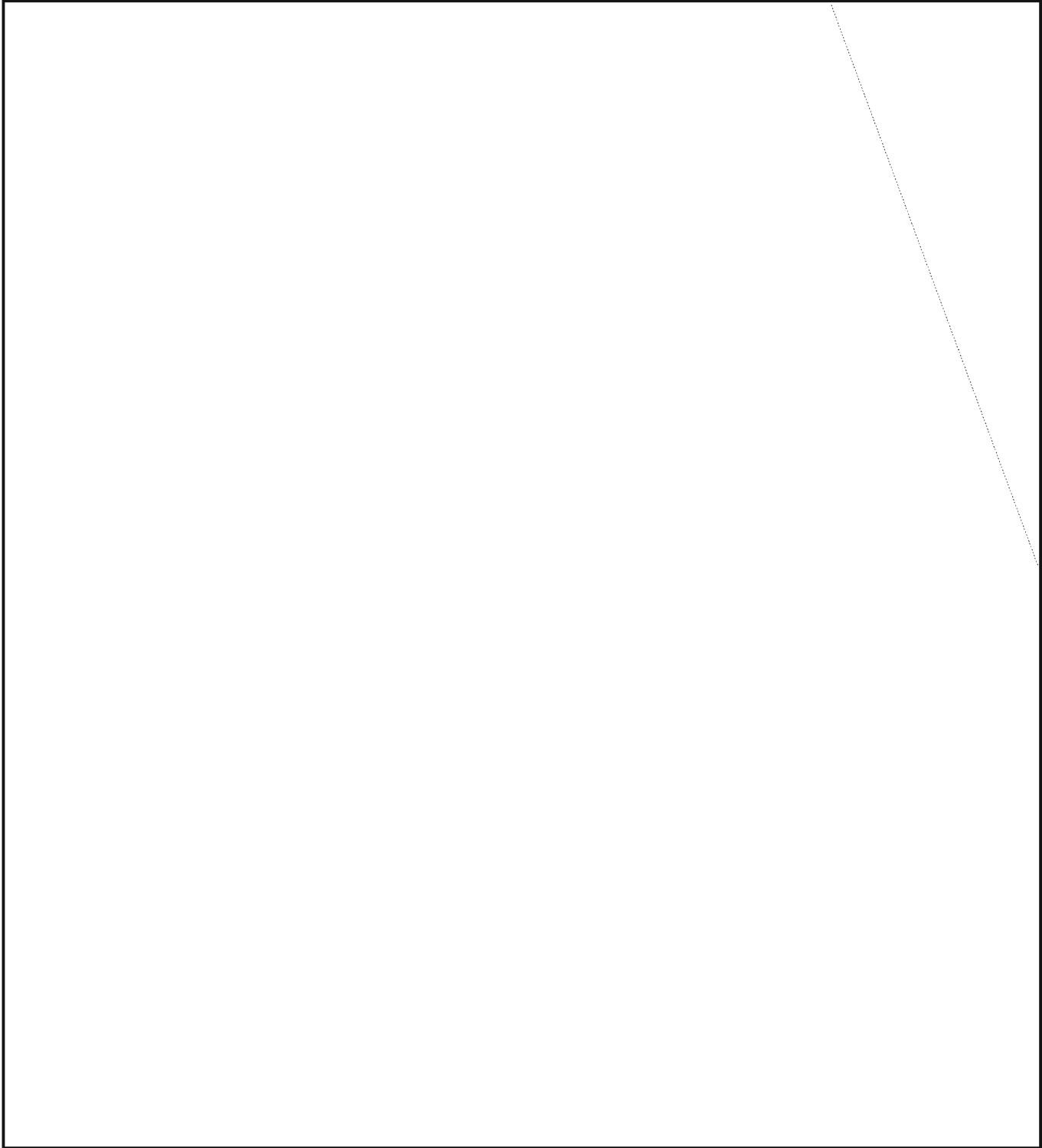
~~TOP SECRET UMBRA~~

~~FOR OFFICIAL USE ONLY~~

T-VISION

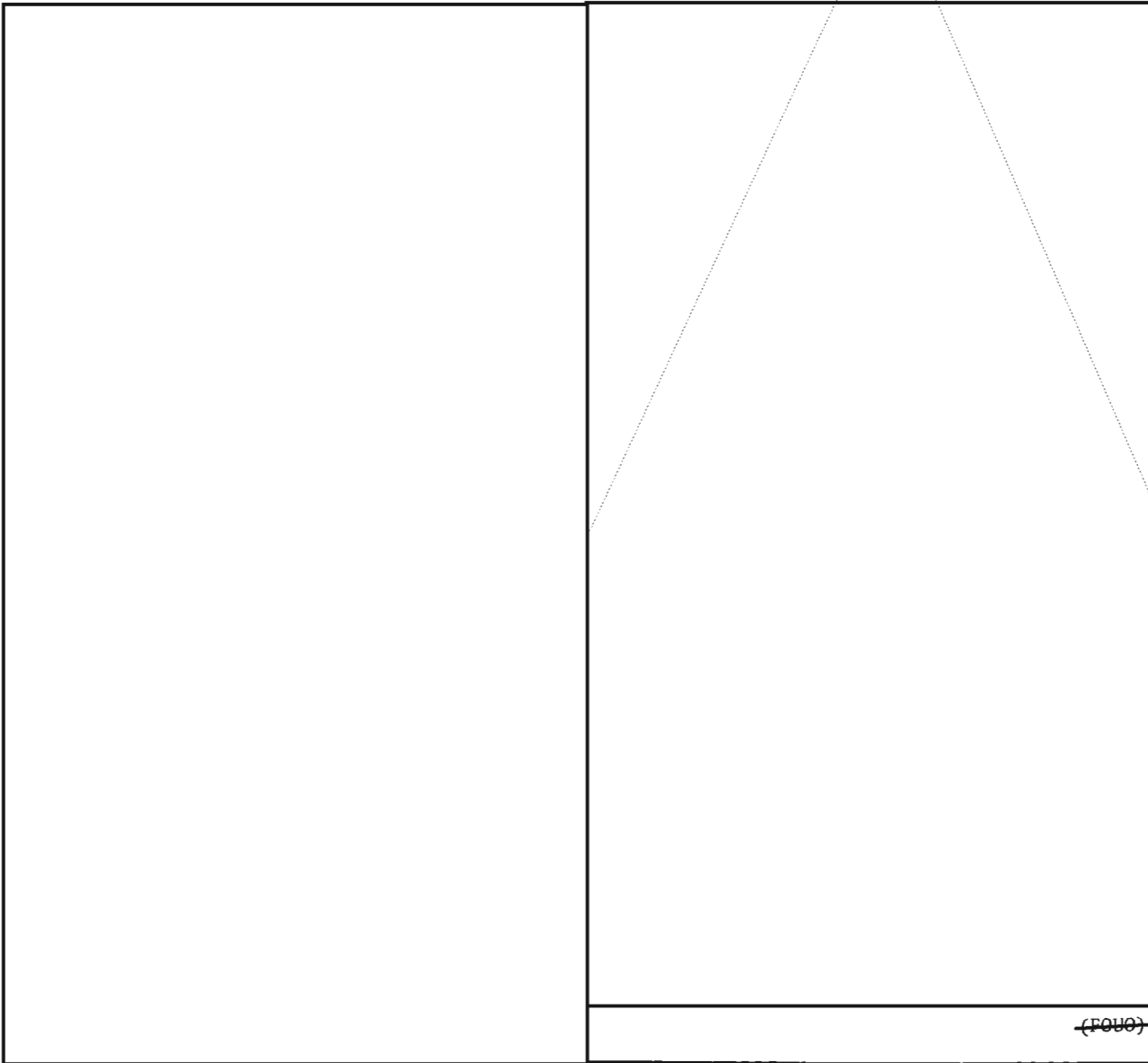
P.L. 86-36

(THE REFERENCE ANALYST'S MEDIUM OF THE FUTURE)



~~FOR OFFICIAL USE ONLY~~

~~TOP SECRET UMBRA~~



(FOUO)



News of the CMI

On 12 October 1978 the Crypto-Mathematics Institute presented the first CMI President's Award to [redacted]. The President's Award is an honorary award established to recognize and honor recent significant contributions to cryptology through the use of mathematics.

[redacted] received this award for his efforts on the cipher machine PENNY/WISE. While on tour at the Institute for Defense Analysis, he created the mathematical description which has been the foundation for [redacted].



The individual plaque and accompanying letter were presented to [redacted] CMI President. [redacted] pointed out that all ten of the submitted nominations represented significant contributions to cryptology and the Agency's mission. [redacted] was chosen from among this select group as the person whose work provided the most significant recent contributions through the knowledge, understanding, and application of advanced mathematics.

Among the many attendees of the party to honor [redacted] and the other nominees were several distinguished guests, including VADM B. R. Inman, Mr. Robert E. Drake, MGEN George L. McFadden, Mr. William Lutwiniak, [redacted] and [redacted].

[redacted] Pl. x3957s (TSC)

~~TOP SECRET UMBRA~~

~~SECRET~~REFLECTIONS AND
RECOMMENDATIONS~~SECRET~~Vera R. Filby,
E41

In March 1978, the Intelligence and Traffic Analysis Division of the National Cryptologic School (E41) and the Reporting Guidance and Quality Control Division of Operations (V12) consponsored a seminar on SIGINT reporting because of increasing awareness in both organizations that general strain on SIGINT reporting was causing local pain. Efforts to alleviate the problems, caused mainly by intensification in recent years of opposing demands on SIGINT producers to provide SIGINT more abundantly and at the same time protect it more stringently, have been attempted throughout the cryptologic community, but treatments applied, often successfully, to ailing parts of the system have caused maladjustments elsewhere. The attendance of some 90 interested participants for two days of the conference showed that concern over this situation is shared by many. Since an account of the conference, *Proceedings of the SIGINT Reporting Seminar, 8-9 March 1978*, has been published and is available (E41, 7119s), this paper will not comment on the events of the seminar but instead offer reflections and (unofficial) recommendations.

Postseminar reflections lead to the pessimistic but predictable conclusion that since March nothing has changed. Hence the "recommendations" are offered with the even more pessimistic conviction that nothing will change -- but offered nevertheless. The recommendations would be hard to carry out because the problems are chronic and their treatment controversial. They are also so interrelated that they could just as well be stated in other ways, and they lead to subordinate recommendations. The main ones are the following three.

RECOMMENDATION: RETHINK THE ENTIRE SYSTEM OF PHILOSOPHY OF SIGINT REPORTING.

Analyze explicitly and exhaustively all the perennial problems: technical information, need-to-know, interpretation, commentary, sanitization, compartmentation. This should be done by a committee of members with a strong and abiding interest in the subject and with real clout -- not a job to be delegated. Only on the basis of doctrine firmly and realistically established can action be taken on the next

RECOMMENDATION:

EO 1.4.(c)
ISOLATE, CONSIDER, AND
RESOLVE ALL PECULIARLY
SIGINT QUESTIONS OF
STYLE.

These questions are not of secondary importance, and they should be solved, every one of them. They are all indispensable for effective guidance to SIGINT producers at all stages of product preparation. The solution to these questions must precede work on the next

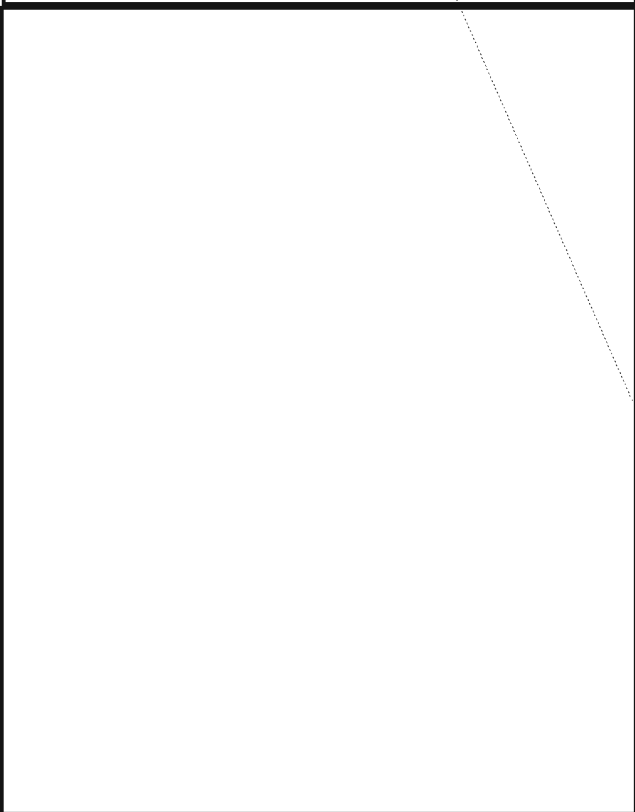
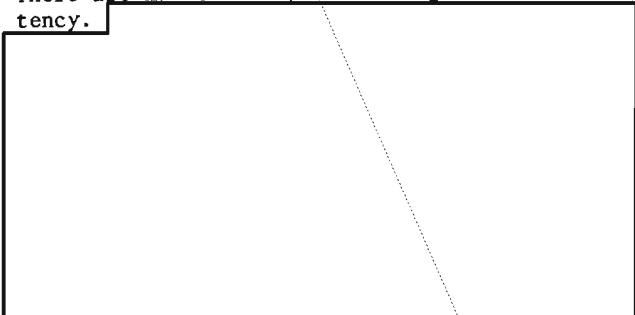
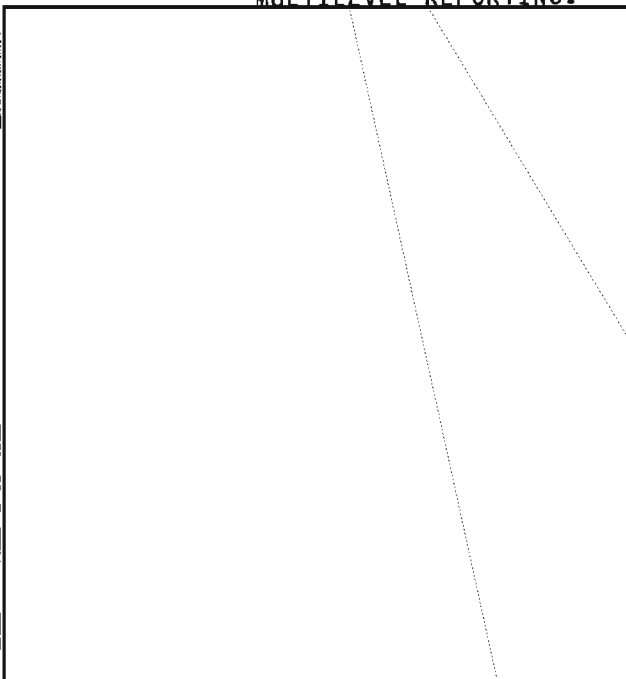
RECOMMENDATION: REWRITE BASIC GUIDANCE, PROMULGATE IT, AND ENFORCE IT.

All basic guidance need not be issued in the same form or at the same time. Easier parts, such as mechanical style rules, can be -- maybe should be -- issued separately.

~~SECRET~~~~HANDLE VIA COMINT CHANNELS ONLY~~

Since obviously all this would require a great deal of effort, it may be well at this point to justify these recommendations. Who needs them? Why? The answer is that everyone in the reporting chain needs them because everyone needs clear, consistent, comprehensive guidance; and for situations that cannot be covered or anticipated with specific rules and guidance, producers at all stages need to understand the principles that inform the system. There are now too many cases of gross inconsistency.

RECOMMENDATION: DEVELOP AND TEST A GENERAL SYSTEM OF MULTILEVEL REPORTING.



RECOMMENDATION: ISSUE TECH SUPPLEMENTS WITH PRODUCT AND MAKE THEM AVAILABLE TO SIGINT PRODUCERS ONLY, THROUGH SOLIS.

SOLIS is the best thing that has happened to SIGINT reporting at NSA since OPSCOMM. It could be even better and more useful than it already is. SOLIS programmers have performed such miracles already that they could surely manage this if policy allowed.

After a recommendation as wildly unlikely to be fulfilled as that one, a much more modest proposal, just a little thing, can serve to end this paper. Someone at the seminar suggested, and everyone -- well, almost everyone -- warmly agreed, that it would be very helpful if NSA product, [redacted]

identified the producing section, this not for credit but for convenience. NSA is a very large organization. Any device to help a reader find the place in it where a question can be answered or an item of information coordinated without going through frustrating and time-wasting sequences of telephone calls would be a boon. So, as a concluding

RECOMMENDATION: MAKE USE OF THE PROFESSIONALIZATION CRITERIA BEING PREPARED FOR THE EDITING AND WRITING CAREER FIELD.

Re-creation of the entire system of SIGINT reporting doctrine is not likely to happen soon, if ever, but meanwhile experimental ideas can be tried. One idea, discussed in detail at the seminar, is summarized in the next

RECOMMENDATION: SHOW THE PRODUCING UNIT ON NSA PRODUCT.

This could easily be done by entering the organizational designator of the producer (A25, G63, etc.) in some convenient place, say the end of the I&A line or following the reference serial. This should be a cinch for SOLIS.

UNCLASSIFIED

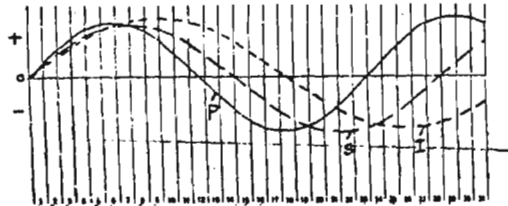


NEWSLETTER

CRYPTOLOG is pleased to reprint in its entirety the September 1978 issue of *Human Factors Newsletter*. The newsletter is published by the CISI (Computer and Information Sciences Institute) Special Interest Group on Human Factors. It is produced "semirandomly" by the Chairman of that Special Interest Group, Douglas Crewell, A635, 3717e/7540b, and is edited by Jeanne Mahoney, W23, 5150e/6255b. Persons who would like to be put on the distribution list for the *Human Factors Newsletter* and to receive other information about the activities of the Special Interest Group should get in touch with Mr. Crewell or Ms. Mahoney.

Ed.

BIORHYTHMS -- EVERYBODY'S GOT ONE. . .



BIORHYTHM CHART PROGRAMMS — Major companies use bio-charts to monitor key employees for their highs-lows and critical days. Available in COSOL, GIBOL and BASIC. Documentation and Program source deck (\$0 cal) supplied. Send \$25 to:

...or for about \$15 you can order a computer-produced "personalized" biorhythm chart; you can buy a calculator that tells your biorhythmic state; or you can drop a few coins in a biorhythm machine at the airport to find out how you should feel today or whether or not you should make or avoid major decisions.

Shades of astrology and snake oil merchants!

What is this "biorhythm" thing anyhow? Seriously -- the biorhythm theory is one of several theories concerning the fluctuations of human behavior. Scientific research (about 3000 papers have been published on the subject) has established that biorhythms are valid and are practically universal in biological organisms. Most people experience rhythmical variations in their physical, emotional, and intellectual states. The chart reproduced above shows the plot of a "typical" biorhythm cycle for each of these states. The numbers along the x axis represent days. It is believed that an individual's biorhythm characteristics can be determined by carefully collecting and analyzing data over a long period of time. This is a complex problem and the biorhythm theory is generally not well understood, so be cautious about what some sidewalk hawker promises you for a small fee.

I have extracted from two recent articles some information that I hope you will find interesting and enlightening:

"There are two views of biorhythms, the popular and the scientific. The popular view is largely fancy and ignores virtually everything that has been scientifically established about biorhythms. . .

". . .the popular theory of biorhythms has been put forth in dozens of books, newspaper and magazine articles, and is followed by many thousands of people. Popular 'biorhythms' are determined solely by one's birthdate. Given this single piece of information, one's biological rhythms are assigned to be exactly determined for one's entire lifetime. This popular theory claims that everyone has a physical, emotional and mental cycle of exactly 23, 28 and 33 days, respectively. No variations are permitted because of differences in sex, age, climate, occupation, or other variables. . .

". . .every published scientific test of this popular theory has shown no correlation between these simplistic cycles and one's true biological rhythms." (M. Lattimer Wright, "Biorhythms: Fact and Fancy," *Proceedings of the Human Factors Society, 21st Annual Meeting, 1977*, pp. 193-196)

Is the biorhythm useful for accident prevention?

"In a continuing effort to predict accident behavior, the biorhythm theory has been used by some researchers as a tool to attempt to bring a degree of logic and order to what remains an otherwise unpredictable situation. . .

". . .For the sample examined in this study, there was no relationship between accident occurrence and biorhythmic criticality. Until some of the inconsistencies of the theory and its lack of precision are eliminated, the use of biorhythm as an accident prevention aid appears to be of no value . . .

"use of more definitive information . . . if combined with more carefully designed research methodology, would eliminate much of the ambiguity observed in present studies and produce more meaningful results." (M. W. Brownley and C. E. Sandler, "Biorhythm -- An Accident Prevention Aid," *Ibid.*, pp. 188-192)

UNCLASSIFIED

Want to read more? Copies of these articles can be obtained by calling me -- [redacted] 3717s/7540b. If my biorhythm cycle is on a "high," I will respond intelligently, rapidly, and very emotionally.

A LATE-BREAKING NEWS ITEM

Mr. Zaslow, DDT, presented a most interesting talk to CISI on 21 September. During the question and answer period, the subject of "Human Engineering" was raised. Mr. Zaslow's response was direct and to the point. He stated that NSA (specifically computer program-

mers and system designers) must do a better job of providing systems that are "friendly" and responsive to user needs. He correctly stated that there is no one at NSA with a job title of "Human Factors Engineer" and no Human Factors organization to turn to for Human Engineering support. In short, Human Factors Engineering at NSA is a failure. We must do all we can to improve man-machine interfaces. Computer systems are user tools -- not ends in themselves.

P.L. 86-36

Such comments are refreshing and very encouraging to those of us who have been waving the Human Factors flag for so long!

A TYPICAL USER CAT AT A TYPICAL (UGH) COMPUTER DISPLAY TERMINAL



IF THE PROGRAMMING CATS READ [redacted] IEEE REVIEW, IT MIGHT GIVE THEM SOME IDEAS ... WE GOTTA DO BETTER ... ///@%##, BURP ... PLEASE STAND BY ... HELLO, USER CAT? THIS IS YOUR COMPUTER ... HELLO!?

Article Review

W23

P.L. 86-36

A recent article in the *IEEE Transactions on Software Engineering* dealt with user-perceived quality of interactive systems. User-perceived quality is defined as a set of system properties which are relevant to man-computer interaction from the user's point of view. User's views vary with the needs, problems, and preferences encountered when assessing software products. User-perceived quality, therefore, is not a distinct quality but rather a multi-dimensional concept.

User data was gathered through questionnaires given to more than 300 experienced users of interactive systems with the Federal Republic of Germany. Data was submitted to several factor analysis procedures, to date mainly applied in psychology but in no way limited to any scientific discipline. In factor analysis, variables are organized into a smaller set of statistically independent linear combinations of variables, so-called factors or dimensions.

UNCLASSIFIED

The emphasis in factor analysis is on understanding the nature and structure of complex measurements through examination of the relationships to a relatively few underlying features.

From factor analysis, seven factors were extracted. They are: 1) self-descriptiveness; 2) user control; 3) ease of learning; 4) problem adequate usability; 5) correspondence with user expectations; 6) flexibility in task handling; 7) fault tolerance. Each factor is composed of a set of requirements belonging together, with factor loadings of at least 0.30; smaller loadings indicate random correlations. The higher the loading, the more important is a requirement with respect to the interpretation of a factor. Also, in looking at the loadings one can see that most requirements have high correlation with only one factor.

It appears that most factors are cognitive in nature. The factor "correspondence with user expectations" additionally addresses affective behavior. Motorial behavior is, if need be, addressed in parts by the factor "fault tolerance."

It may seem surprising that some qualitative aspects such as performance and responsiveness do not appear in the framework. These might appear, however, if some of the factors were substructured. However, this process would require much more research and empirical verification.

The article also discusses the statistical analysis, made to determine the validity and reliability of the factors. The authors hope that this is a step toward more user-oriented interactive systems where users access the systems and designers are guided to translate user-oriented criteria into the specifics of particular system design.

Factors of User-Perceived Quality

Factor 1: "Self-descriptiveness"

- 0.70 explain system requests to the user if and when necessary
- 0.68 supply explanations in different detail and different format upon user request
- 0.67 supply help features pertinent to any dialogue situation
- 0.60 enable transparency of dialogue organization and dialogue sequence at any time
- 0.52 explain each command and subcommand upon user request
- 0.45 give clearly arranged presentation of system functions
- 0.45 supply interactive programming aids which provide guidance for structured programming
- 0.33 give decision aids if tasks cannot be executed as desired
- 0.33 provide global information about the functional range of the system
- 0.32 make user thoroughly acquainted with system usage without human assistance
- 0.31 by prompting, provide user guidance for the dialogue
- 0.30 supply information about the current system status if desired

Factor 2: "User Control"

- 0.60 admit interruptions of a task to start or resume another task
- 0.59 admit process canceling without detrimental side effects

- 0.59 allow abortion of particular dialogue steps or processes
- 0.48 have a command language syntactically homogeneous
- 0.47 be permanently available
- 0.42 immediately detect syntax errors
- 0.37 permit clustering of commands with a new name
- 0.37 by prompting, provide user guidance for the dialogue
- 0.36 allow user to make background processes visible
- 0.34 supply information about the current system status if desired
- 0.33 have a command language easy to understand and easy to apply
- 0.32 supply comprehensive debugging aids
- 0.31 give decision aids if tasks cannot be executed as desired

Factor 3: "Ease of Learning"

- 0.63 make user manuals superfluous
- 0.61 facilitate the learning of system use without consulting manuals
- 0.57 be usable without special DP-knowledge
- 0.52 largely offer on-line forms for user input
- 0.49 be able to present user manuals in whole or in parts via display station
- 0.41 make user thoroughly acquainted with system use without human assistance
- 0.41 provide global information about the functional range of the system
- 0.41 make the least assumptions about user's prior knowledge of system structures and functions
- 0.40 support user input by menu technique
- 0.33 give error messages with correction hints
- 0.34 explain each command subcommand upon user request
- 0.32 enable the learning of system use without referring to comprehensive texts stored

Factor 4: "Problem Adequate Usability"

- 0.69 have a data management system that obviates as far as possible the need for the user to perform clerical or house-keeping activities
- 0.63 manage formatting, addressing, and memory organization without bothering the user
- 0.56 determine system decisions without consulting the user
- 0.50 accept free formatted command input
- 0.44 have a command language easy to understand and easy to apply
- 0.42 be tolerant towards erroneous user input
- 0.41 have a syntactically homogeneous command language
- 0.38 have a command language easy to remember
- 0.32 make repetitive or routine input unnecessary

Factor 5: "Correspondence with User Expectations"

- 0.76 behave similarly in similar situations
- 0.71 request analogous user actions to similar tasks to be performed
- 0.65 offer minimum astonishment behavior towards the user
- 0.37 let user recognize effects of his input
- 0.34 be tolerant towards erroneous user input
- 0.33 enable transparency of a dialogue organization and dialogue course at any time
- 0.31 provide same response times to equal activities

Factor 6: "Flexibility in Task Handling"

- 0.56 allow user to extend the command language
- 0.55 allow facilities for stacking tasks
- 0.47 allow user an arbitrary access to the task stack
- 0.44 provide system messages with different levels of detail dependent on user status
- 0.42 provide reduced input/output according to user's training level
- 0.41 allow user to define his set of system functions
- 0.35 provide shorter ways for trained user to perform his tasks
- 0.35 permit user to define some particular user status
- 0.34 allow user to make background processes visible
- 0.32 permit clustering of commands with a new name

Factor 7: "Fault Tolerance"

- 0.53 insist only on partial retyping if previous input was erroneous
- 0.52 tolerate typical typing errors
- 0.49 give error messages with correction hints
- 0.40 enable user to submit concatenated commands as input
- 0.35 accept reduced input when actions are to be repeated
- 0.34 give error messages in full text
- 0.32 give decision aids if tasks cannot be executed as desired
- 0.31 support user to find his way

UNCLASSIFIED

NSA-croctic No. 21

By David H. Williams, P16

The quotation on the next page was taken from an article that appeared in an NSA publication. The first letters of the WORDS spell out the author's name and the title of the article.

DEFINITIONS

WORDS

- A. NFL team (2 wds) 239 47 31 174 60 82 121 106 225 42 161 152 56 165
248 25 114 89
- B. Where the season ticket-holder can be found during any home game (3 wds) 197 146 100 185 79 243 211 199 33 49 39 237
- C. Saw 68 12 58 156 97 108
- D. "All the rams are chasing ____; They're determined there'll be new sheep..." (Rogers and Hammerstein, "Carousel") (2 wds) 138 191 219 158 194 155 202 4
- E. Untanned cattle skin; old TV series 128 149 209 154 81 67 102
- F. Former NFL star, played himself in film biography "Crazy Legs," 1953 (2 wds) 90 48 77 172 193 137 32 96 198 13 120
- G. High-altitude Asian capital city (2 wds) 250 101 207 176 133 119 8 200 217 164
- H. Did a grease job (slang) 201 244 84 92 95
- I. N. Calif. structure, a major component of San Francisco's water supply system (3 wds) 214 30 46 110 242 212 236 177 86 75 103 168 41 226
- J. Competitor in any sport or physical activity 159 125 192 151 206 21 129
- K. Trump 70 167 52 173
- L. Conducted an incursion or foray 232 189 118 59 123 99
- M. "Letting 'I dare not' wait upon '____' ____ the poor cat i' the adage" (Macbeth) (3 wds) 1 196 204 111 134 223 228 6 20 215
- N. Baer or Schmeling 72 144 230
- O. Income Tax Day (3 wds) 181 139 179 249 105 213 91 34 78 11 241 93
- P. NFL team whose home stadium is at Foxboro (2 wds) 222 66 188 26 62 160 208 14 44 183
- Q, Sharp, repeated knocking or tapping sound (comp) 122 163 166 127 142 94 187 136 104 203
- R. Period or state of decline (2 wds) 229 150 234 184 240 205 69
- S. Team for which Word F played (2 wds) 145 233 141 130 2 83 195 135 16 247
- T. NFL team (2 wds) 98 63 251 107 64 37 124 27 3 235 74 22 218 190

UNCLASSIFIED

U. NFL team (3 wds)

36 221 112 227 18 76 186 71 23 88 245 148 157 50
162 65 5 116

V. In the same place (Lat)

210 17 51 132 169 15

W. Noontime sign on the boxer's door (3 wds)

43 73 171 115 178 28 54 182 19 57

X. Major work by Anton Dvorak (3 wds)

131 85 117 220 109 29 7 61 153 180 40 231 246 53
170 143

Y. NFL team (2 wds and comp)

45 87 35 80 24 147 55 126 175 238 224 140 10 9
113 38 216

1 M	2 S	3 T	4 D	5 U	6 M	7 X	8 G	9 Y	10 Y	11 O	12 C	13 F	14 P	15 V	16 S		
17 V	18 U	19 W	20 M	21 J	22 T	23 U	24 Y	25 A	26 P	27 T	28 W	29 X	30 I	31 A	32 F		
33 B	34 O	35 Y	36 U	37 T	38 Y	39 B	40 X	41 I	42 A	43 W	44 P	45 Y	46 I	47 A	48 F	49 B	
50 U	51 V	52 K	53 X	54 W	55 Y	56 A	57 W	58 C	59 L	60 A	61 X	62 P	63 T	64 T			
65 U	66 P	67 E	68 C	69 R	70 K	71 U	72 N	73 W	74 T	75 I	76 U	77 F	78 O	79 B	80 Y	81 E	
82 A	83 S	84 H	85 X	86 I	87 Y	88 U	89 A	90 F	91 O	92 H	93 O	94 Q	95 H	96 F	97 C		
98 T	99 L	100 B	101 G	102 E	103 I	104 Q	105 O	106 A	107 T	108 C	109 X	110 I	111 M	112 U	113 Y	114 A	
115 W	116 U	117 X	118 L	119 G	120 F	121 A	122 Q	123 L	124 T	125 J	126 Y	127 Q	128 E	129 J	130 S		
131 X	132 V	133 G	134 M	135 S	136 Q	137 F	138 D	139 O	140 Y	141 S	142 Q	143 X	144 N	145 S	146 B		
147 Y	148 U	149 E	150 R	151 J	152 A	153 X	154 E	155 D	156 C	157 U	158 D	159 J	160 P	161 A			
162 U	163 Q	164 G	165 A	166 Q	167 K	168 I	169 V	170 X	171 W	172 F	173 K	174 A	175 Y	176 G	177 I	178 W	
179 O	180 X	181 O	182 W	183 P	184 R	185 B	186 U	187 Q	188 P	189 L	190 T	191 D	192 J	193 F			
194 D	195 S	196 M	197 B	198 F	199 B	200 G	201 H	202 D	203 Q	204 M	205 R	206 J	207 G	208 P			
209 E	210 V	211 B	212 I	213 O	214 I	215 M	216 Y	217 G	218 T	219 D	220 X	221 U	222 P	223 M	224 Y		
225 A	226 Y	227 U	228 M	229 R	230 N	231 X	232 L	233 S	234 R	235 T	236 I	237 B	238 Y	239 A	240 R	241 O	242 I
243 B	244 H	245 U	246 X	247 S	248 A	249 O	250 G	251 T									D.H.W

(Solution next month)

UNCLASSIFIED

UNCLASSIFIED

DEPARTMENT OF GOLDEN OLDIES

ON FIRST OPENING KENNEY'S "STATISTICS"

Marjorie Mountjoy (RETIRED)

[redacted] E42, found this unpublished item among material he inherited, through [redacted] from Marjorie Mountjoy when she retired a few years ago. CRYPTOLOG reprints it herewith in its original form, without even changing its title to "Statistics, Don't Be Mean to Us Cryppies!" Ed.

The trouble with *Statistics* was that I don't think I survived the definition of "the mean" (p. 32 ff.).

It was stated three times; in the conventional "compact" notation, and it was all supposed to amount to the same thing:

$$(1) \bar{x} = \frac{1}{N} \sum_{i=1}^N x_i$$

$$(2) \bar{x} = \frac{1}{N} \sum_{i=1}^k f_i x_i \quad (\text{where } N = \sum_{i=1}^k f_i)$$

$$(3) \bar{x} = \frac{1}{N} \sum_{i=1}^k f_i (c u_i + x_0)$$

As any fool can plainly see from the left-hand side! It was the right-hand side that bothered me.

Now it is not the mathematics, because, to get the mean, you simply take the total and divide by the number of items, so it must be the language. So the thing to do is to learn the language, in case the next time you have to do something, it may be something you do not know how to do already.

O.K.

" \bar{x} " (I think it is pronounced "ex-bar") stands for "the mean." "N" is the total number of variates (and a "variate" is defined as "the magnitude of a variable," see p. 7). So that brings us up to " \sum ," pronounced "sigma," because "sigma" is "S" in Greek and what it means is "Sum" (impera-

tive) -- starts with "S" -- get it? This, as the book tells you, is a sort of mathematical verb, also known as an operator, and the notation written above and below it are adverbs, otherwise known as *limits*. It cannot but follow, for one with any imagination at all, that the " x_i " or the " $f_i x_i$ " (where

P.L. 86-36

$$N = \sum_{i=1}^k f_i \text{ or the "f}_i\text{" (c u}_i\text{ + x}_0\text{) part,}$$

which the book calls the variates, are actually *nouns* in the *objective case*, *direct objects* of the verb " \sum ," and by this time I am so entranced with the grammatical structure of the equations that I want to diagram them and to find out whether, being part-Greek, they are inflectable. It is difficult to get back to mere mathematics, but this flight of syntax leads nowhere. Therefore, "i" is the "index of summation." "Any letter may be used, but it is conventional to use *i* or *j*." "Frequently the index of summation is understood from the context, and the notation at top and bottom of \sum may be omitted if no ambiguity results." I have found, in actual practice, that omitting all forms of the "index of summation" from the equation *cleared up* the ambiguity in 99 cases out of 100.

This just about covers our examples. No -- wait! That "u" in equation (3) is in case you don't have time for the regular procedure for computing the average and want to take a short cut. It is defined as:

$$u = \frac{x - x_0}{c}, \quad (c \neq 0).$$

"c" represents "units," and " x_0 " is the "new origin" (see "translation of axes," p. 35); " \neq " I believe I remember to mean "is not"; "k" of course is explained in (2) as:

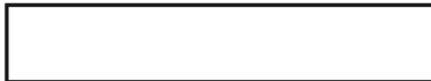
$$N = \sum_{i=1}^k f_i.$$

This makes it all very simple, I suppose. Really, as I say, I sort of faded out at this point.

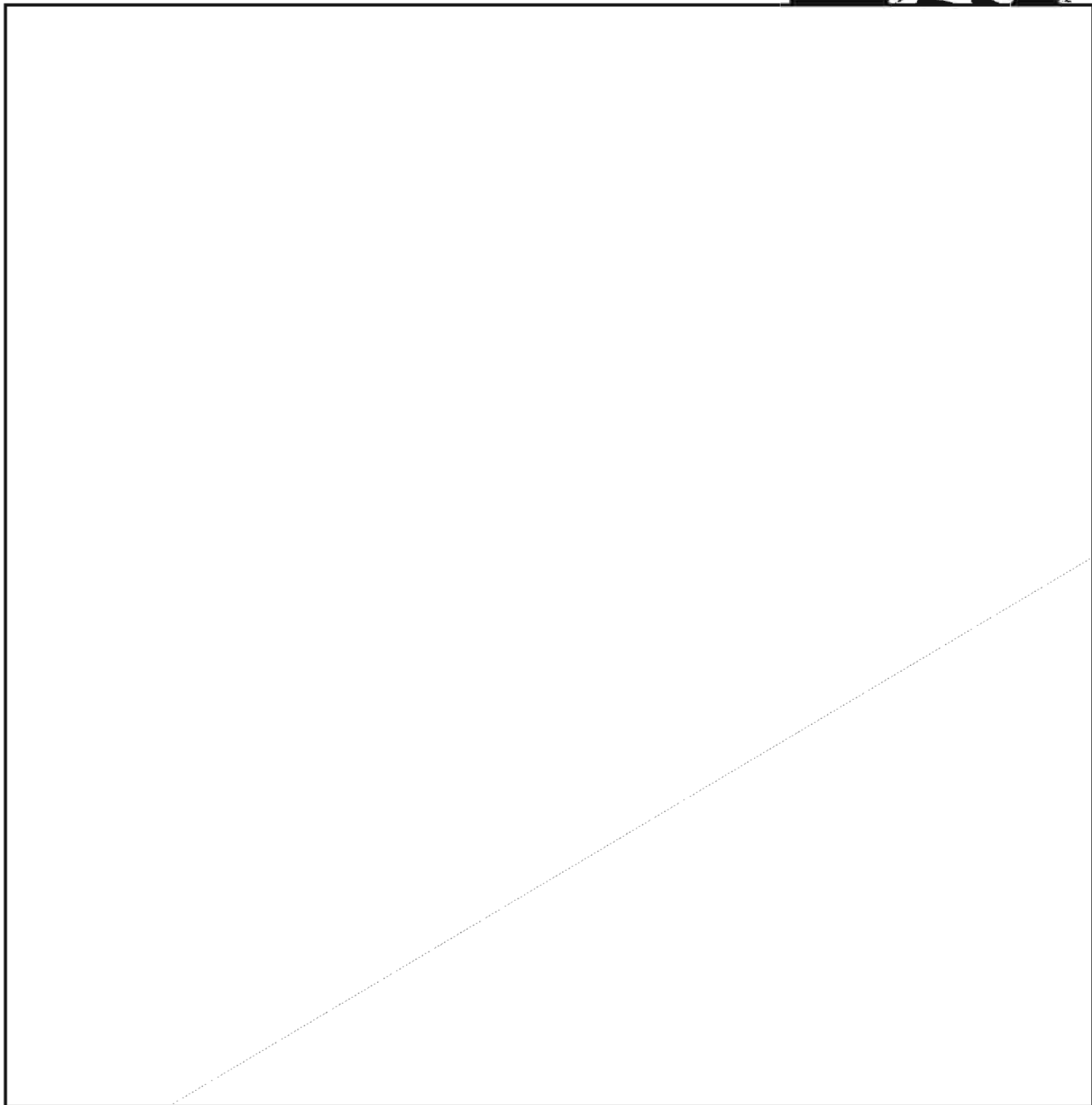
(U)

UNCLASSIFIED

*HENRY CEMENT
AND OTHER PHANTOMS
OF THE OPERA(TIONS)*



G51



CLASSIFICATION CORNER

CLASSI-

"IT'S PARTY TIME!"



[Redacted]

DDO Classification Advisory Officer

P.L. 86-36

Have you classified a party lately? How about a "Second Party" or a "Third Party"? It's time we classified all parties the same. The following information may help.

In the past, the terms "Second Party" "Third Party" (instead of actual country names) were used in an attempt to keep the references unclassified or at the lowest possible classification level. The old rules, which were never documented, but which were used by me and other classification officers, were:

Sample references	Appropriate classification
Vague references to "Second Party" and "Third Party" organizations, even though mention of SIGINT and COMINT may have been included.	U
References to "Second Party" and "Third Party" in such a way that they revealed we were referring to a country other than the United States (e.g. "Third Party country").	C
References to the specific country when COMINT was stated or implied.	S-CCO

New guidance specifies that the terms "Second Party" and "Third Party" in a SIGINT or COMINT context will be classified "Secret -- Handle Via Comint Channels Only." Examples of references and their appropriate classification under the new guidance are:

Sample references	Appropriate classification
"Direct liaison with Second and Third Party organizations is not authorized."	S-CCO
[Redacted]	S-CCO
[Redacted]	S-CCO

[Redacted]

S-CCO

S

U

References to "Second Party" or "Third Party" which are made in a COMSEC context, whether stated or implied

Considering the above guidelines, it may be beneficial to mention the actual country or countries involved in your correspondence, rather than vague references to "Second Party" or "Third Party." The sample statement starting "Direct liaison..." could be changed to "Direct liaison with GCHQ and [Redacted] representatives

is not authorized." The classification is S-CCO in both cases, but the statement is much more informative when the specific countries are mentioned.

The guidance contained herein is from the Director's Policy Staff and should be used uniformly throughout the Agency. It will be reflected in forthcoming regulatory documents, including the NSA/CSS Classification Manual and USSID 3.

~~(S-CCO)~~

THIS MONTH'S

Letters to the Editor



(U)

**Chief P1
Office of Techniques and Standards**

- 27 November 1978

Art Salemme, the second editor of CRYPTOLOG, retires in January. He has brought along the lusty youngster conceived and raised by Doris Miller to healthy, mature status. CRYPTOLOG, thanks to Art's indefatigable promotion, no longer staggers from issue to issue. There is now a modest, but actual, backlog of articles to help in planning ahead. Under Art's editorship the newsiness and readability of CRYPTOLOG have improved. His uninhibited way with headlines and illustrations has enhanced its liveliness and saucy appeal. He has handled controversy with wit and tact. Above all he has kept the content useful and relevant, informal but informative. He has served us well. We wish him a happy productive retirement, and hope to keep a string on him so we can reel him back in for his linguistic talents when occasion warrants.

William L. Twinn
Publisher
CRYPTOLOG

During my career at the Agency I've done a lot of interesting things (in and out of the Handicraft Club), but the years I've spent since my elevation from the position of CRYPTOLOG Art Editor to that of Art, Editor easily qualify as my high three. I've had a lot of fun hustling articles, telling potential authors "Let's you and him fight!", and slapping their articles into print, sometimes providing them with a slightly impertinent illustration or title in order to lure someone into reading an article he or she might have otherwise passed over. I've had *my* fun, but why be greedy? Why not let someone else take a crack at it? So, I'm pleased that Dave Williams (see P. 6) is r'arin' to go. Give him all your support with articles, letters to the editor, suggestions, etc., and he'll make CRYPTOLOG better than ever!

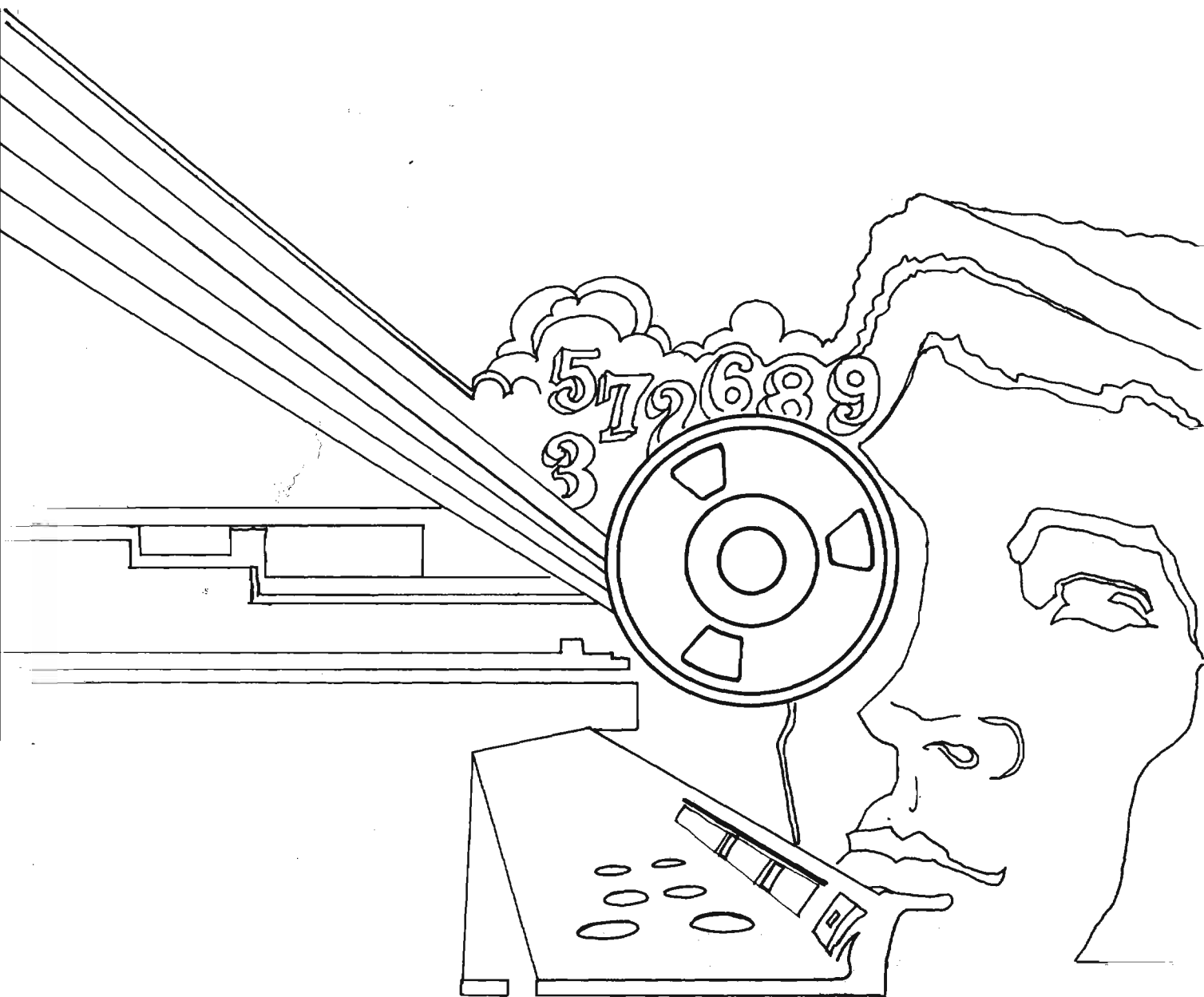
art,

Al Balloni, Editor



(U)

~~TOP SECRET~~



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~