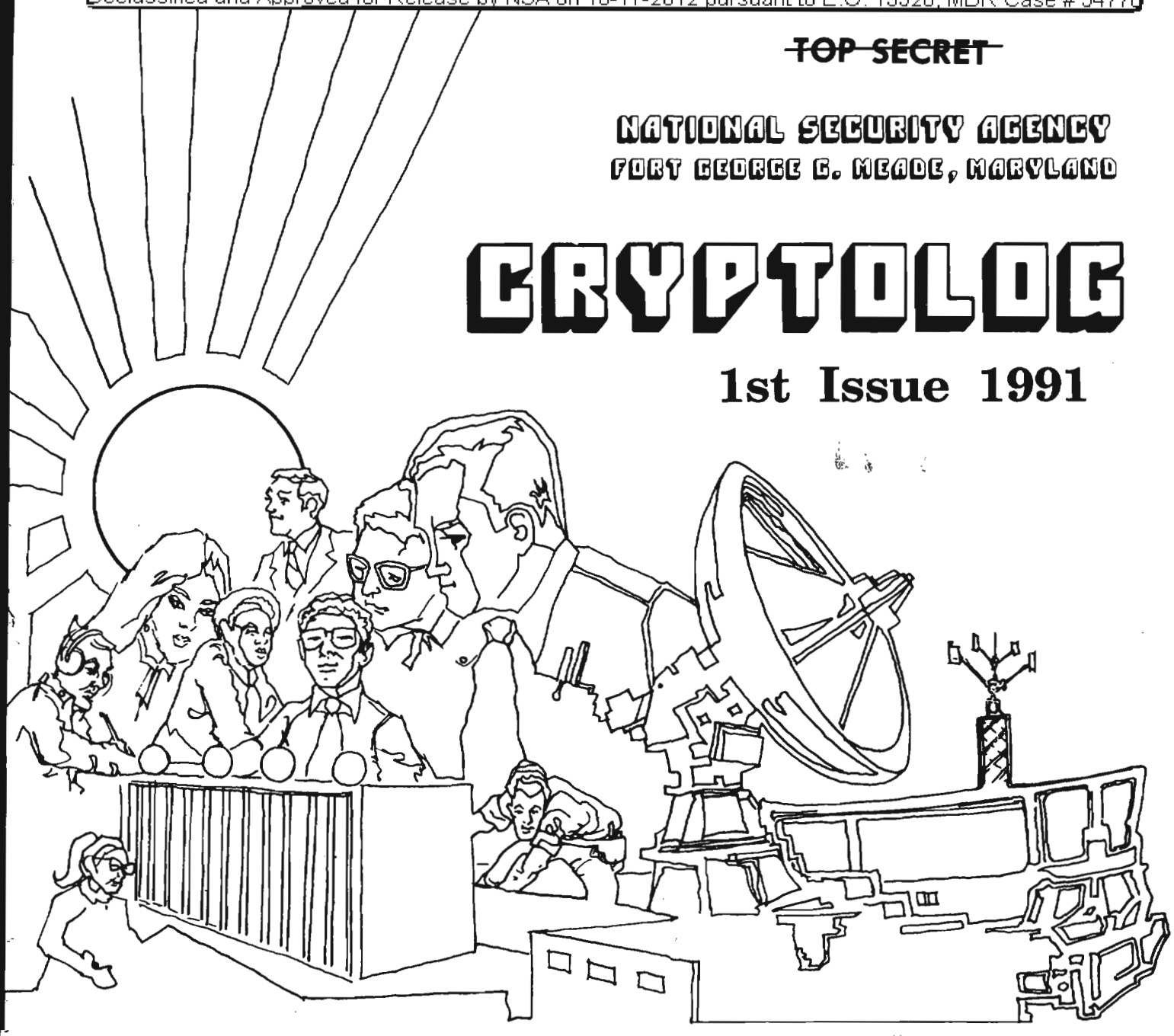
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

1st Issue 1991



P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

~~NOT RELEASABLE TO CONTRACTORS~~

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XVIII, No. 1 . . . . . 1st Issue 1991

To submit articles and letters, please see inside back cover.

For New Subscription or Change of Address or Name

MAIL name and old and new organizations and building to:

Distribution, CRYPTOLOG, P1, NORTH
or
via PLATFORM: cryptlg @ barlc05
via CLOVER: cryptlg @ bloomfield

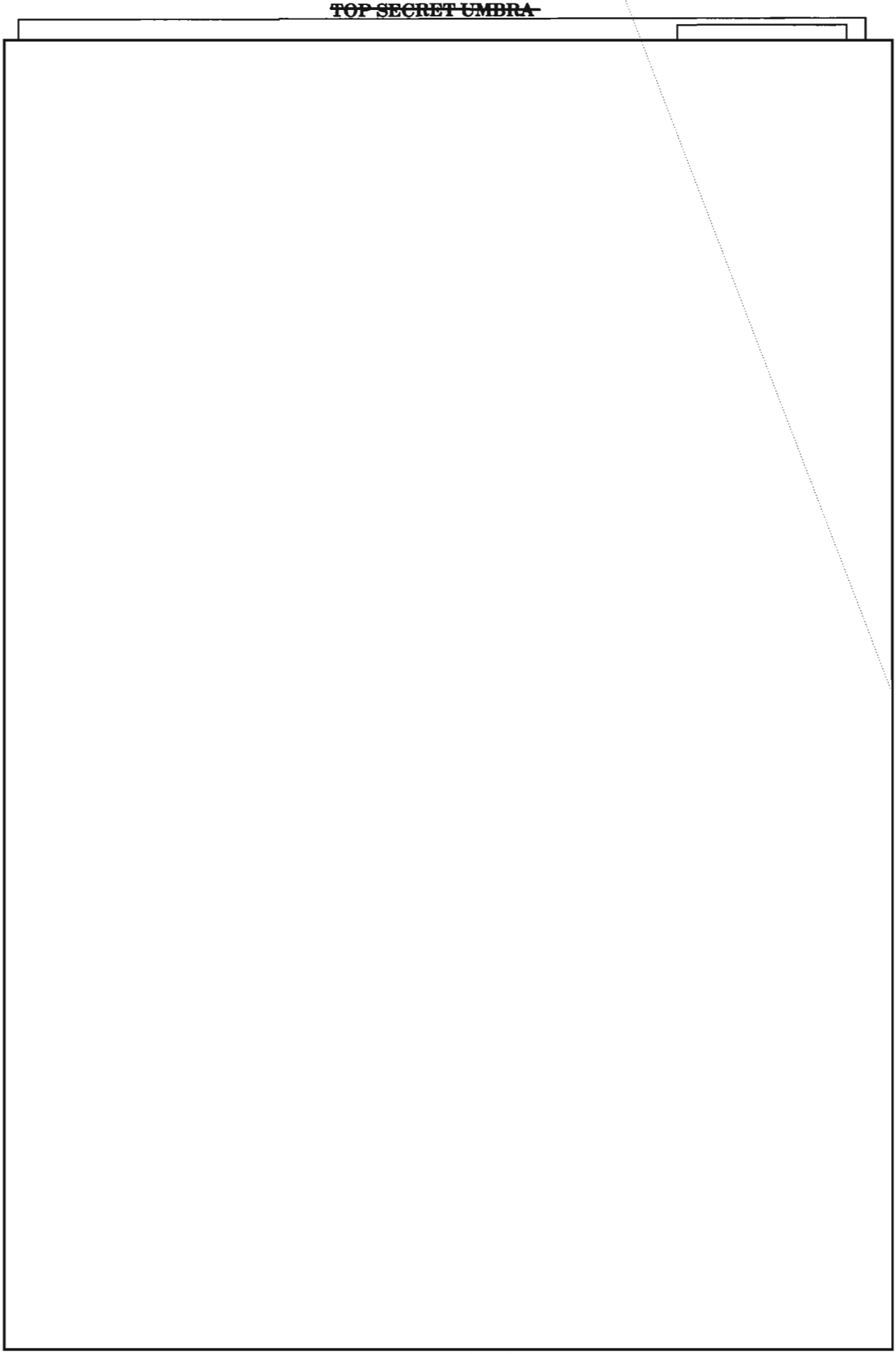
Please do not phone about your subscription

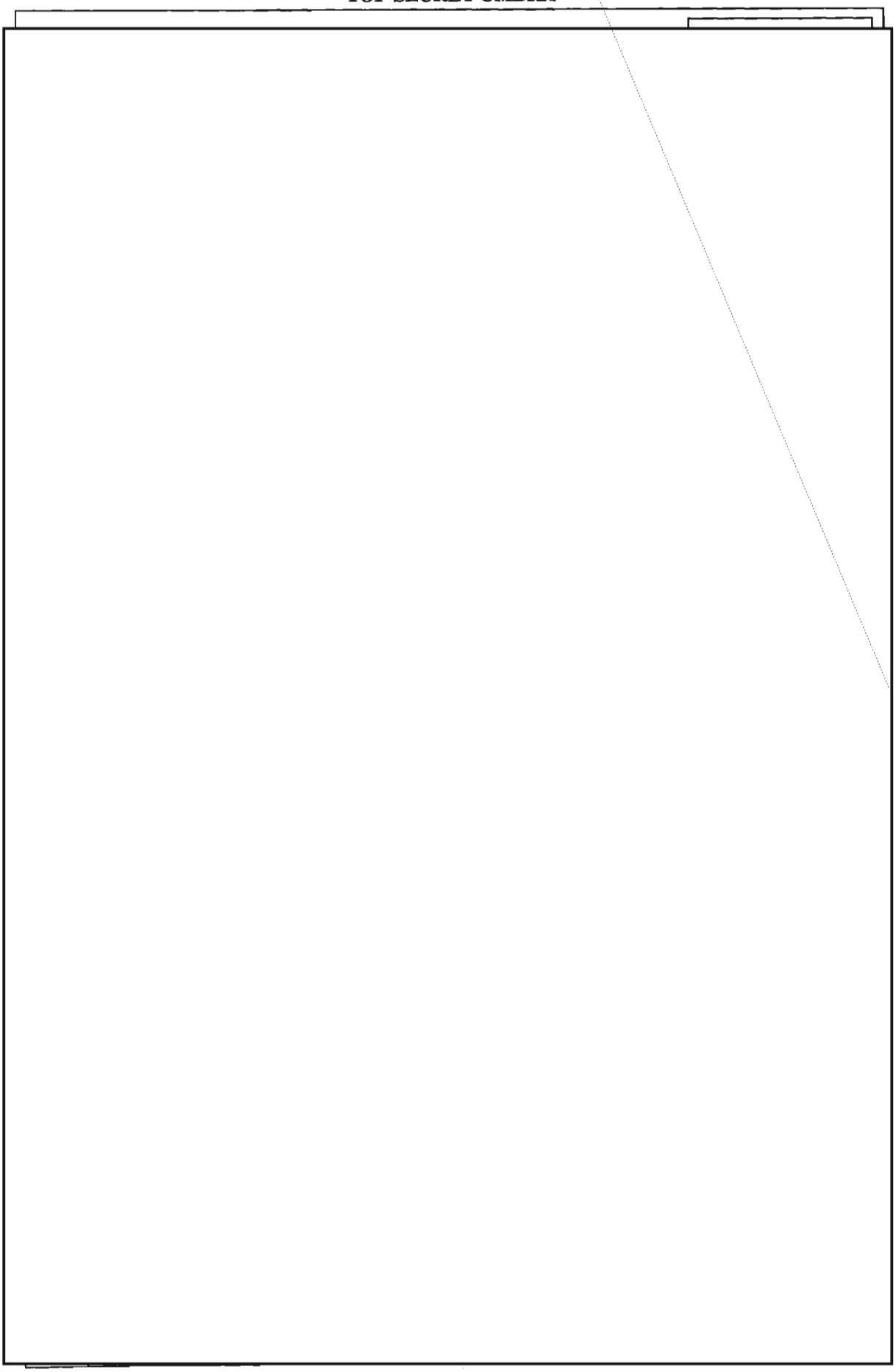
All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

~~FOR OFFICIAL USE ONLY~~

GISTER

G52 P.L. 86-36





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

P.L. 86-36

- 50 -

At an informal ceremony held in P1 on 5 February 1991, a small group met to commemorate the passage of 50 years since Bill Lutwiniak started to ply his arcane trade of cryptanalysis in the sanctuary of the organization–now NSA–that was founded on, and is nurtured and sustained by this discipline.

Bill retired in 1981 and has worked as a reemployed annuitant since then. He continues to make significant contributions as a consultant to P1, solving systems himself, and more importantly, assisting our younger generation of cryptanalysts. Bill served for many years as chief of A5, then of P1, and is a distinguished member of both Kryptos and the Crypto-Mathematics Institute.

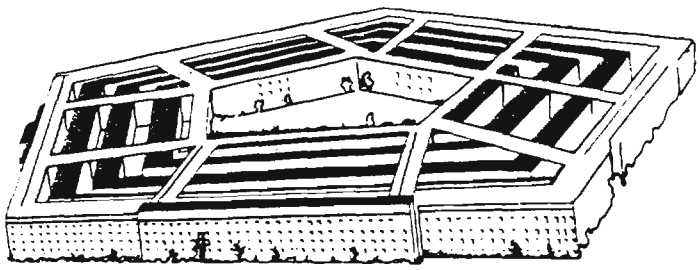
At the ceremony a crossword puzzle (elsewhere in this issue) was presented to Bill, turning the tables on this well-known cruciverbalist.

Later this year a series of interviews with Bill, conducted by [redacted] will be released on videotape.

[redacted]

~~FOUO~~

~~SECRET~~



J O I N T—The Future of Intelligence? Y O U B E T !

(U) Picture this; A room full of analysts representing practically every intelligence element located anywhere in the Washington area and beyond; folks from NSA, DIA, AIA, AFIA, NOIC, NPIC, ITAC, SRD, ESC but none from CIA or KAOS. Uniforms from the Army, Navy, Marines, and Air Force, all side by side with civilians mixed among them. PC word processors on many desks, volumes and volumes of relevent textual materials all brought together by the individual who believed that it was needed "just in case", and more map boards with push pins, acetate overlays, boundary lines, and arrows than anyone could have followed intelligently anyway. Secure phones and STU-III's next to each other. Classified conversations in this hectic environment in the background of calls home. Fax machines that are tempermental, and open phone lines to the various commands in Saudi Arabia. Clocks set for other parts of the world with all their minute hands pointing to different minutes. A few small fans blowing stale air around staler bodies. CNN monitors of various sizes in different parts of the room without logic to their placement. With these 24-hour operations, nothing was turned on and off, except the copier when the new one was worn out and it was replaced with the other new one. Got the picture?

(U) I have just completed my assignment at the Joint Intelligence Center (JIC), Pentagon, in support of the Secretary of Defense and the Chairman, Joint Chiefs of Staff during the DESERT SHIELD and DESERT STORM Operations. I came away from there with a very good understanding of how all the different intelligence agencies contribute to the Joint Operations INTelligence (JOINT) picture. More importantly, I became aware of how this agency is perceived by others and how attitudes affect our validity and how knowledge affects attitude. P.L. 86-36

(U) I was in the first group of people selected for duty at the Joint Intelligence Center in August '90. That first Saturday when we all met was surely a hectic day. And, right from the start, it was evident that NSA had sent its best. By afternoon, the original dozen of us were dubbed Weasels" USN was in charge of the group), an enthusiastic group eager to get to the task.

(U) We all attended many meetings We were even briefed on

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~ 1.4.(c)
P.L. 86-36

the other wars in the area. Thanks to the professional experts at NSA who had prepped us, we arrived at JIC very well informed. Getting the necessary working aids, phone numbers, and office supplies was very reminiscent of a scavenger hunt. A tour of the JIC facilities, still under construction, and the Pentagon badging processes completed our preparations.

(U) The Sunday of Labor Day weekend 1990 was the first day on the job in the JIC. I was first on the ground desk which I thought was appropriate anyway since I was the only Army person on the NSA team. It also allowed me to set many of the desk policies and procedures used throughout the lifespan of the JIC. There were a few growing pains as each member rotated through the desk for the first time. But, being true professionals, we adjusted. The "housekeeping"—arrangement of files, desk areas—was better than I expected, and the equipment held up remarkedly for the abuse we gave it. Transportation to and from the Pentagon was provided for us and was truly a life saver. George and Steve, our drivers on the night shift, were especially friendly, courteous, and safe.

(U) In the first few days of the DESERT SHIELD operations, when the Joint Intelligence Center was a newborn, organized chaos was the best descriptor. People from all these different agencies were just coming together, sizing each other up, establishing boundaries, assuming roles—all the routines that surface when two or more clans come face to face. Shy and quiet would eliminate you from the team discussions. If you wanted to be a part of the team, you had to push into it. Once that was done, however, you were in for life. Duties were created as they were deemed necessary. Division of efforts were naturally established based on the most likely source of the information required. The NSA desk was responsible for all the SIGINT material, the imagery guys for imagery, etc.

[redacted]

[redacted]

Participants in JOINT

AFIA: Air Force Intelligence Agency
AIA: Army Intelligence Agency
DIA: Defense Intelligence Agency
ESC: Electronic Security Command
ITAC: Intelligence and Threat Analysis Center, AIA
NOIC: Naval Operations Intelligence Center
NPIC: National Photo Interpretation Center
NSA: National Security Agency
SRD: Special Research Division, ITAC

(U) Each team in the JIC had its own personality. Of course, I like to think that the team I was on was the best. The only real problems I saw were personnel changes and role definitions. No one on the desk really understood what the NSAer's role was as a part of the team. I envisioned my role as a key player in the

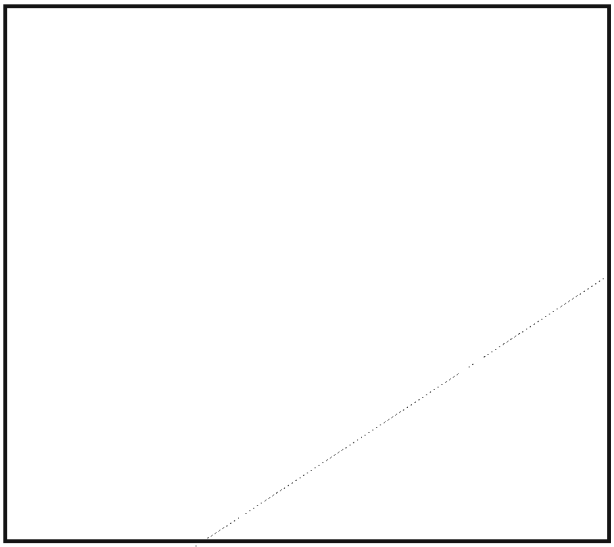
[redacted]

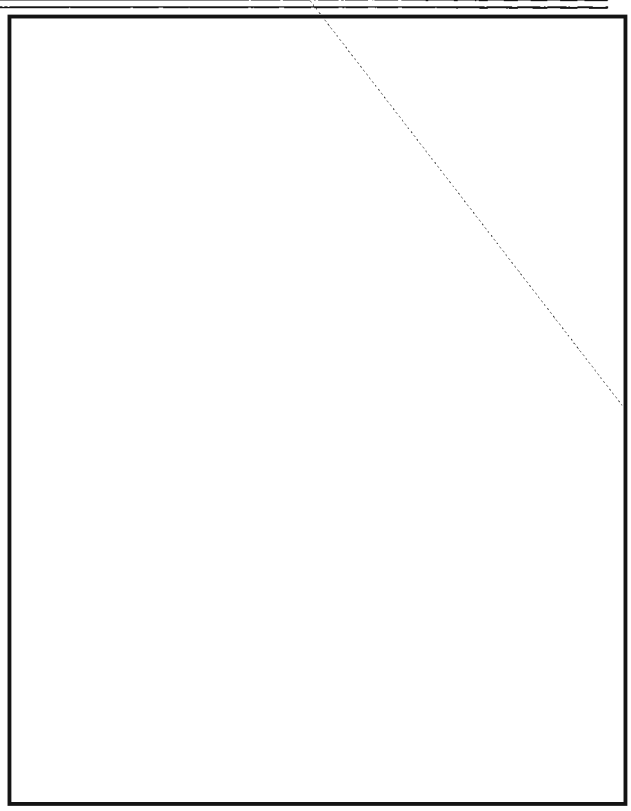
This last duty is what all the other members of the team thought my job was until they were convinced otherwise. [redacted] I had to insert myself into the whole team again. But, after awhile, I was able to steer some discussion and even successfully suggested tasking, based on my SIGINT and JOINT understandings. This tasking provided positive results, too. I never felt at any time that anyone on the team was overly interested in the technical aspects

the Klieglights coming over the NTSS. But, it was helpful to me to have them. I could speak my native SIGINTese to the NSA ground forces analysis team based on the tech details I had seen in the KLIEGLIGHTS.

~~(C)~~ The mission, as it grew on the Ground Team was to provide all-source intelligence estimates to Rear Admiral McConnell, the intelligence officer answering to GEN Powell and to Secretary Cheney. All source meant all source, too. It also meant that efforts would have to be combined. A joint effort from each of the intelligences was needed. Not only that, based on these efforts, a reasonable assessment of what happened, what is happening, and what will be happening, by whom and when and how and etc, had to be presented each morning to the Admiral. Also we provided support to military operations directly in theater at Riyadh, Saudi Arabia.

(U) Wisely, two only routine reporting vehicles were established, rather than the many one might expect. One was the Military Situation Summary. This was designed to keep the field elements apprised of the current order of battle and the JIC's assessment of events relative to the order of battle. The other regular publication, the Defense Special Assessment, published significant tactical and strategic intelligence. This vehicle had a much more limited audience and was sometimes focused for the Washington area alone.

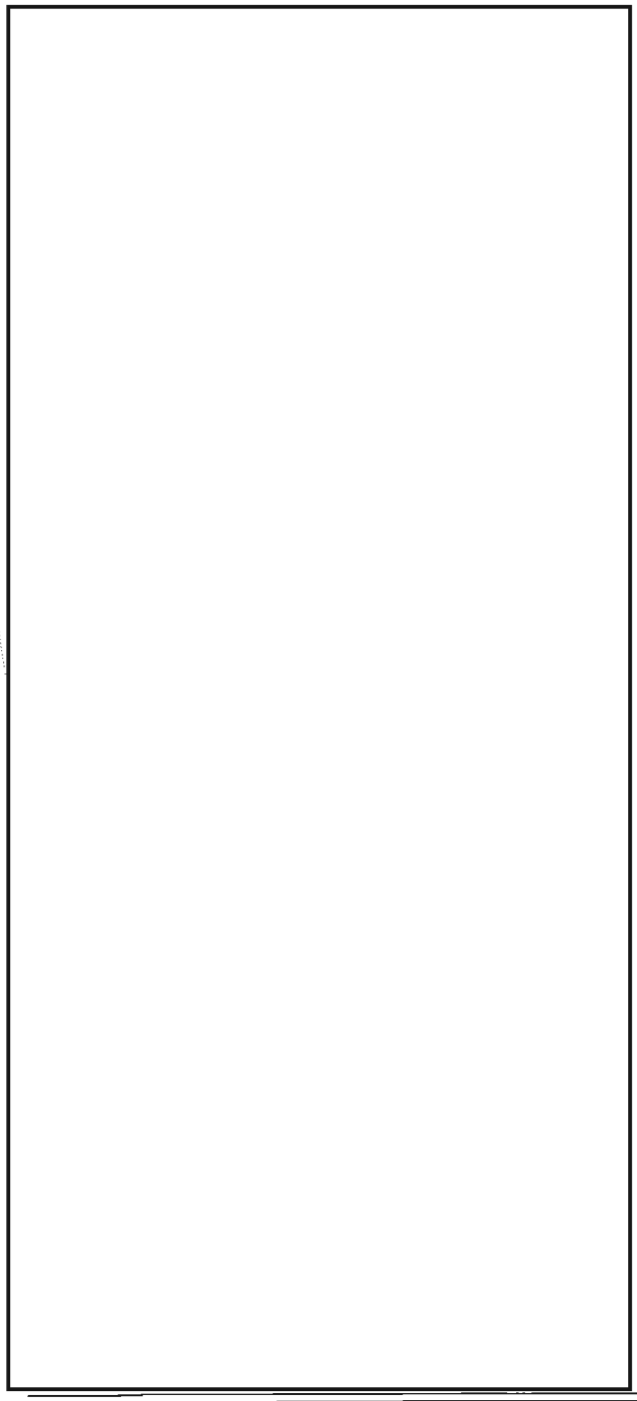


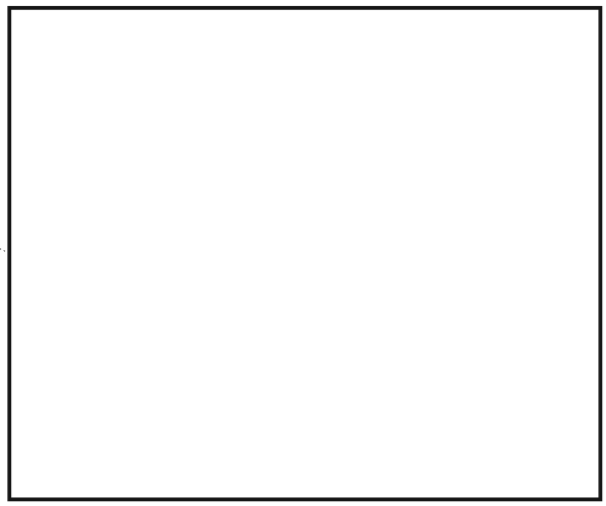


(U) In a matter of minutes, usually, all the national-level intelligence in the community could be brought to bear in a cohesive, complete, and conclusive picture for the warfighters and decision makers "upstairs". There was little interaction with parent agencies. No one at NSA had to say "Wait till the day shop comes in and we'll get you an answer." The same held true for every other agency. The around-the-clock operations and the on-hand expertise from all the different agencies could usually handle the task quickly and efficiently. I really believe that this type of operation was a key element in the successes in joint operations planning and in theater, and because of it, we contributed significantly to the field commander's nearly instant knowledge of the battlefield immediately in front of him.

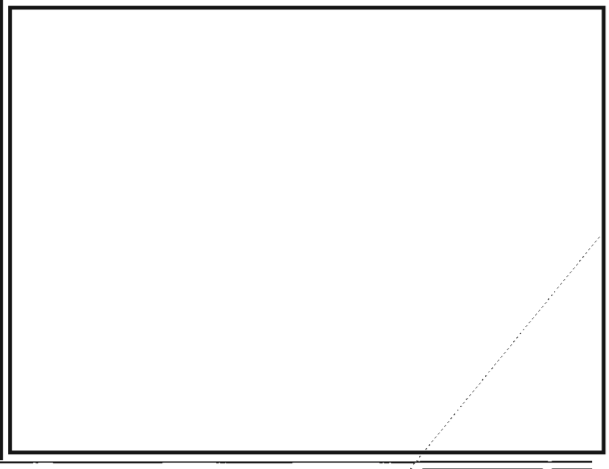
~~(FOUO)~~ From time to time, my connections with "the fort" were tested. At the beginning, I had carte blanche access to the NSA ground desk just as the Director had intended. Then, for some reason, that was nearly choked out and without warning. I discovered later that the choking of access came from a single source, and that soon

was obviated. At least with most of the military members on the desk, my rank helped to keep lines open. The sergeants did not really want to tell the warrant officer that they were not permitted to talk to him. (Good choice on their part.) Don't take me wrongly, there were many professional analysts who understood the magnitude of the mission and readily assisted in spite of some of the inane management directives.





~~(FOUO)~~ Back to JOINT— **J**oint Operations **INT**elligence. JOINT provides probably the quickest, all-source analysis of events to the national decision-makers. And it does it very well. The down side of what the JIC could do dealt mostly with the classification sensitivities, especially for SIGINT. Reports that were ORCON often contained the most usable intelligence for the field commanders, except that the field commanders couldn't receive the reports. Attempts at stripping out the relevent parts and removing ORCON caveats was almost always a time-consuming, thankless chore. But we did it. We also got angry when the field reported an ORCON TACREP in their summary as SECRET Releasable to Multi-National Forces. Yes, that happened, too. There were moments, in the heat of the battle as they say, when your conscience made the ORCON release decision for you. Then the paperwork followed.



agency represented and an appreciation for the process of producing finished intelligence at those agencies. What we did was take all the work of many many people and consolidate it, encapsulating for the folks "upstairs" the meat of the matter in a complete picture. What each of us did was provide our own expertise in the intrepretation of products for those who may have incorrectly intrepretated or misread a product. My many explanations of how the SIGINT processes work changed attitudes and that, in turn, changed the validity factor.

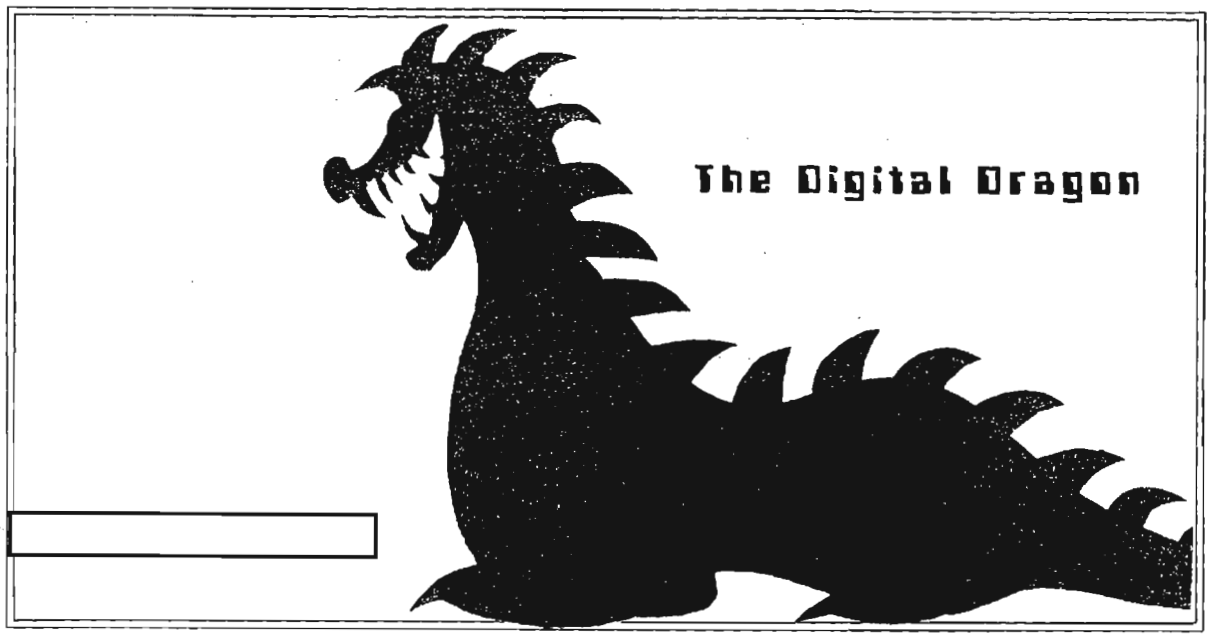
(U) In light of the huge successes of Operation Desert Storm, what happened in this first-of-its-kind JIC probably indicates the future of intelligence for the battlefield and definitely for Pentagon and the White House. I think many of us agree that future conflicts will necessarily be joint service, if not combined national, ventures. And the one in charge of these ventures will have to be well versed in the intelligence community and its capabilities. It was smart to put the JIC together and the JIC provided tons of information where and when it was needed. An intel-smart General or Admiral could appreciate the JIC response to his needs and temper it appropriately in his planning. The use of national resources real-time during warfare operations can often provide a broader perspective and analysis of current events than a smaller, less equipped, more narrowly focused, in-theater service asset can provide. And the JIC proved it could be done with very good accuracy and timeliness. I do not believe the JIC portends the demise of our individual organizations, merely it enhances the intelligence they produce and provides a complete nationally derived, usually more sensitive, intelligence information for our leaders to respond to today's fast-paced, short-fused decision requirements.

(U) Finally, I very much enjoyed serving in the JIC and feel I did contribute to our victories. It wasn't as sandy as the gulf, but I'd bet it was just as arduous. I have been in the Army for over 20 years. I always felt, especially in the intelligence fields, my mission was not to wage war, but to preserve peace—prevent war. I started my career in the Army in Vietnam. I am ending my military career as this war ends. As I look back, I wonder if I have done my job to keep the peace. The successes of this war and the miniscule number of casualties would suggest that our intelligence was right on—that I did do my job and did it well. However, this euphoria is hazy. What would have happened if the enemy really wanted to fight? I never want my brother and my nephew who served in the Gulf to know. Nor do I want my son to know in the future wars. I want the next JIC to be just as succesful, if not more so, in providing the politicians the ammunition they need so we, as a nation, do not need to provide ammunition to servicemen and women.

BULLETIN BOARD

SOUTHEAST ASIA AND VIET NAM ~~(S-CCO)~~

~~(S-CCO)~~ The Center for Cryptologic History, D9, is attempting to locate surviving materials pertaining to Southeast Asia and Viet Nam, whether official records or private holdings. The massive destruction of records in the mid-1970's has left significant gaps in the record of our efforts, especially VH/VC. If you know of any material about our efforts in this region—records, working aids, etc.—please notify D9, Ops 2B, 963-7292.



P.L. 86-36

(U) The People's Republic of China (PRC) has undergone a revolution in its telecommunications field within the last five years. This resulted from the decision to become a formidable world economic power early in the 21st century, with help from industry in Europe, Japan, Australia, and the United States. But industry of the developed world found that communication via telephone or telex was hampered by outdated and overused switching and transmission equipment. Nothing could be done until the many services involved in the complex chain of modern industry could "talk" to one other. This meant that an integrated telecommunications system had to be established quickly, including modem-connected computer-to-computer data transfer, telex, and business facsimile traffic, and be interfaced efficiently with the international telecommunications system through gateway facilities via communications satellite services and international undersea cables.

(U) Telecommunication was accorded a very high priority in the Seventh Five Year Plan (1986-1990) and has contined to remain so in the Eighth Five Year Plan (1991-1995). Innovation will be required to modernize to world standards.

(U) The Ministry of Posts and Telecommunications (MPT) is the primary center for telecommunications standards, long haul interprovincial systems, communications research, and equipment production. But each province and each Ministry is responsible for establishing its own standards, equipment purchases, and telecommunications structure. Except for the People's Liberation Army (PLA), all entities are to use European (CEPT) standards. The PLA, which does not need to meet international standards for its telecommunications needs, initially adopted a 512 kb/s mobile troposcatter system (TS193) and subsequently standardized with 460.8 kb/s mobile microwave (204A) and troposcatter (GS207 III) for flexible strategic communications requirements.

(U) The MPT has the telecommunications engineering and production expertise needed to support its function. Through the mid 1980's the Chinese used FM/FDM equipment almost exclusively; however, since 1988 microwave radio relay lines serving Beijing-Tianjin, Beijing-Shijiazhuang, and Beijing-Shanghai (including route cities Jinan, Xuzhou, and Nanjing) are being connected using CEPT Level 4 PCM (140 mb/s) equipment. Current planning provides for major Level 4 microwave lines to connect Beijing with most of the provincial capitals in the populous eastern and the industrial central portions of the

country by 1995. Most of the provinces have installed and are now operating digital microwave systems interconnecting the key nodes within their borders. East-West cross connection between Chengdu and Shanghai will be accomplished using multimode optical fiber cable, portions of which are currently under construction. In addition, a national digital 300-baud telex system using V.26 standard was initiated in the Spring of 1989. This telex system is replacing the older stacked Voice Frequency Telegraphy telegram systems, long the mainstay of PRC record traffic.

SWITCHING CENTERS

(U) The wealthier coastal provinces, because they are more involved with foreign business, moved rapidly to modernize their telecommunications. Indigenous production of digital telecommunications was limited mainly to smaller size Level 1 and Level 2 equipment or to small PBX switching systems. Some Level 3 microwave equipment was produced but its quality was considered poor in comparison to Japanese, American, and European products. The microwave routes were established, towers constructed, and antennas bought in-country. The digital telecommunications equipment was imported.

~~(S-CCO)~~ A modern telecommunications structure begins with a fast, flexible, digital telephone switching system. The current standard in advanced industrial nations today is the Digital Stored Program Control (DSPC) switch. This form of telephone switch is electronic and controlledby software. The combination provides the necessary flexibility to allow adjustments as conditions change, as well as the electronic speed to handle large volumes of telephone traffic. Cost of the switch is initially expensive, 150-300 USD per line, but over its life it is cheaper to operate than electromechanical equipment such as crossbar switches. An extremely important consideration is that DSPC switching capability is critical for an Integrated Services Digital Network (ISDN), long the hoped-for dream of the telecommunications world. As the technology to produce the large public DSPC switches did not exist in the PRC, both provincial and private networks have to import them. Among the equipments imported are: FETEX-150, Fujitsu, Japan; DMS-10/DMS-100, Northern Telecom (NT), Canada; AXE-10, L. M. Ericsson (LME),Sweden; System 1240, Alcatel, France; (NEC), Nippon Electric Corp.; NEAX-61, Japan; EWSD, Siemens, W. Germany; 5ESS, American Telephone & Telegraph.

(U) In addition to selling full switches to PRC customers, Fujitsu, and Alcatel established Joint Ventures to produce the components of their switching systems in the PRC. Fujitsu based its (FETEX-150) software support Venture in Fujian Province and Alcatel bought out the Shanghai based Bell Venture, Shanghai Bell Telephone Exchange Manufacturing Corporation (SBTEMC) to produce System 12 (System 1240) switches.

(U) Principle consumers for the DSPC switch market in the PRC include provincial and city level PTA/B's, the MPT, the Civil Aviation Administration of China (CAAC), the various electric power regional authorities, the railroad (MOR), and the People's Liberation Army (PLA). The PLA, although not a large scale buyer, is listed because it is a user on any systems established by the other functions.

(U) As of the date of this report, all provincial capital cities and a number of large prefecture capitals have installed one or more DSPC switches into their telephone structure. The initial entry was made by the Japanese companies Fujitsu and NEC. They had a good sales infrastructure within China and provided their products at a lower cost per line than European, American, or Canadian companies. Fujitsu was particularly successful, greatly aided by its Joint Venture in Fujian province. The Japanese, however, had delivery delays caused by stringent export license regulations. As the money for telecommunications dried up, companies who were able to swing the necessary long-term, low interest rate soft loans became more competitive. Even where the soft loans were available

in Japan, however, the long delivery time caused many Chinese customers to look elsewhere. Owing to these factors, the Canadian firm, Northern Telecom is in a good position for marketing its DMS-100 line.

[redacted]

Provincial Post and Telecommunications

(U) The manner in which the individual provincial Post and Telecommunications Authorities or Bureaus upgrade their telecommunications is dependent upon the degree of industrialization, the desire to attract foreign investment, the percent of the population in an urban or rural environment, the wealth of the province, and the innovativeness of the leadership. As discussed above, the initial step has been to establish a core system using digital Stored Program Control Switches in the provincial capitol and key large cities.

[redacted]

SUMMARY

(U) The infusion of digital technology into PRC telecommunications over the period 1986-1990 has progressed at a rate probably surpassing any other major country. Progressing from having one Level three (34 MBs) microwave line operational between 1981 and 1985, the PRC now has Level three and Level four microwave lines operating in most provinces and state of the art digital SPC switching systems in place and operational for most major cities. Telegrams are now routinely passed through a nationwide digital 300-baud Telex using V.26 modem. Connectivity has been established with world digital standards in the gateway cities via IntelSat and the way is being rapidly paved towards an ISDN environment within the next five to ten years if desired. In terms of telecommunications, the digital world is happening now in the PRC.

(U) **China is truly becoming a Digital Dragon.**

Ich spreche Deutsch

or

Wie ist ihr toiletten?

P.L. 86-36

[redacted] M312

Back in the olden days of 1971, I took a Permanent Change of Station (PCS) assignment to Stuttgart, Germany. My sponsor picked me up at the airport. That day she taught me the word „neun". If you know your eins, zwei, drei, you know that „neun" is German for nine. By stepping up to the reception desk at the Vaihingerhof and trying to make my lips form that unfamiliar word, I was able to get the key to Room #9. That room—Zimmer #9—would be my temporary home until I found an apartment.

As you can imagine, knowledge of this one German word did not afford me an easy passage throughout Deutschland. During my tour in Germany, fortunately I increased my vocabulary. I took German I and II offered on post through the overseas division of the University of Maryland. I also took several German conversational courses. With the knowledge gained from these courses, I was able to order meals at restaurants; reserve a room while travelling and determine if the room was with or without Bad (bath), and if it included Fruehstueck (breakfast), etc.

After awhile I was also able to recognize when German was used incorrectly. I went to dinner with a friend one evening. During the course of the evening, my friend asked the waitress, „Wie ist Ihr Toiletten?" The waitress graciously gave him directions to the men's room. On his way back to our table my friend was grinning sheepishly because he realized that he had used the interrogative wie instead of wo. In so doing, instead of asking "where" the lavatory was, he had instead asked the waitress "how" her lavatory was.

Once on a German bus trip to Italy, my fledgling German language ability came in handy. The German bus driver (who spoke no English) and the tour guide (who spoke fluent German and English) got into a spat. For days they would not talk to each other, but instead communicated through me. It was somewhat hairy at times, but nonetheless a challenge.

I am sure that many NSA employees who have been on PCS assignments have similar humorous experiences with the language of the country. Indeed, I was totally unprepared linguistically for my first experience on foreign soil.

Now, many years since my PCS, I am happy to say that the Office of Personnel provides language tapes to PCSing families. Often there just isn't time to attend a language class before you PCS no matter how well-intentioned you may be. As anyone who has been PCS knows, there is a myriad of concerns about your field tour: where will you live; what will the job be like; what about schooling for your kids. All of these changes are traumatic enough without compounding your discomfort by being unable to speak, read or understand the language.

As most of our lives become busier, more complicated and often plagued by traffic, language tapes can fill a void. By popping a cassette into the car tape deck, you have an opportunity to learn a language during your daily work commute. Why not have a "leg up" by at least learning some of the basics of the language, such as, yes, no, please, thank you, etc. Then when you are approached by someone who asks you, „Wo ist der Bahnhof?", you can competently say, „Rechts um die Ecke, dann geradeaus".

So, if you are processing for an overseas assignment, don't forget to ask the personnel in M31, Field Staffing and Personnel Administration, about the language tapes. The following tapes are available from M31:

[redacted]

Auf Wiedersehen, Viel Glueck, and Prosit!

A Matter of COMPRESSION

P.L. 86-36

P11

COMPRESSION

(U) The compression algorithm we are discussing is to be embodied in a new type of modem, the V.42. CCIT standards for the V.42 have been approved and a number of companies have committed to building their version of it. The British firm HAYES already has a V.42 modem on the market.

(U) The impetus for the V.42 was the rapidly advancing state of the microelectronics art. Industry realized that small, relatively cheap modems could be built with a capability to perform complex functions requiring a high compute and large storage capacity. The V.42 does its own framing and employs an effective error detection and correction by retransmission procedure.

(U) Because the V.42 can ensure that virtually error-free data is received, a "lossless" compression algorithm was selected to be incorporated in the modem. Unlike "lossy" compression algorithms which are error-tolerant, successful decompression by this "lossless" compression algorithm, known as V.42 bis, requires that the data received be exactly that which was sent. The V.42 bis is adaptable, an advantage over most compression algorithms, which are designed to compress a specific kind of data. In the latter case, if the data differs from the type for which the algorithm was designed, performance of the algorithm suffers greatly.

(U) In the V.42 codebook (more generally referred to as a "dictionary") the entries are made dynamically, representing character strings that occurred earlier in the current transmission, so V.42 bis adjusts automatically to the nature of the data being sent. If the modem is used for an Italian language transmission, for example, the dictionary will fill mainly with entries that represent character strings that occur with a relatively high frequency in Italian. If an

accounting report is sent, most entries will represent number strings, row or column labels, or other items in the report format. While the compression ratio achieved by V.42 bis is a function of the roughness of the data being transmitted, it is not affected by the type of data. This versatility, together with its relatively low price and small size is likely to make the V.42 attractive for a wide variety of communicators.

(U) The CCIT standards for the V.42 are flexible enough to allow manufacturers to build models of the modem that range from "stripped down" to "full bells and whistles." Maximum dictionary size may extend from 512 entries to an unspecified upper limit. Maximum string size, i.e., the greatest number of characters that may be represented by a codeword, may range from 6 to 250. Modems with differing capabilities will be able to communicate with each other. At the beginning of a transmission, the corresponding modems automatically "negotiate" parameters. Each proposes a maximum dictionary and string size. In each instance, the low bid wins since the modem with the greater capacity can adjust to the lesser parameter proposed by the inferior modem.

(U) At the beginning of a transmission, the dictionary contains 259 entries. Codewords 0 to 2 are reserved for control functions. The remaining 256 codewords represent the characters of the transmission code. Each character is assigned to the codeword that is 3 greater than its transmission code value. (The expected transmission code is ASCII. Since A = 65 in ASCII, Codeword 68 would represent the one character string A.) These initial 259 entries, known as "root nodes," constitute the fixed portion of the dictionary.

(U) The number of bits transmitted to represent a codeword is the least number needed to convey the value of the last entry in the current dictionary. At the beginning of a transmission, the last entry is codeword 258, requiring nine bits to represent as a binary number. As the transmission proceeds, the dynamic portion of the dictionary begins to fill. When an entry is made for codeword 512, the number of bits transmitted per codeword jumps to 10 because at that point, the dictionary contains an entry whose codeword value cannot be represented by 9 bits. Later in the transmission when an entry is made for codeword 1024, the bits sent per codeword increases to 11, etc.

(U) During a transmission, the compression algorithm looks at the consecutive characters to be communicated. Each time it adds a character to the string it is currently processing, it checks the dictionary to see if it contains an entry that represents the current string. If it does, the algorithm adds the next character to the string. If it does not, the algorithm outputs the codeword that represents the current string minus the last character added and creates a new dictionary entry that represents the current string (including the last character). If the dictionary is not yet full, the codeword assigned to this new entry is the next one available. (If the last entry in the current dictionary is 1000, the new entry will be assigned codeword 1001.)

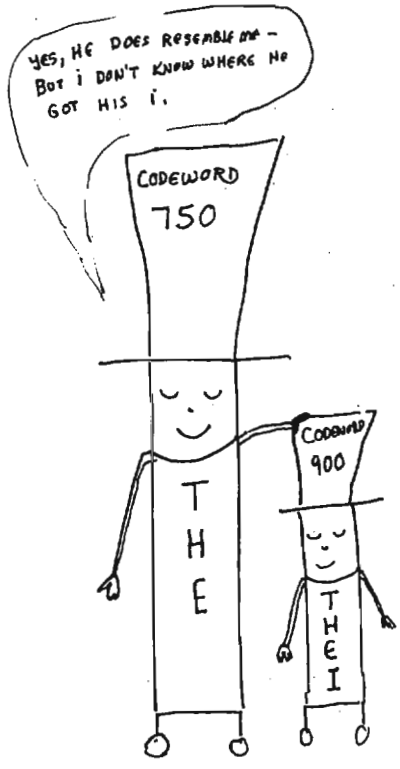
(U) Say, for example, that the first two characters to be communicated are **AR**. The algorithm would first check the dictionary to see if there is an entry that represents the single character **A**. There is. The initial dictionary contains an entry for each of the characters in the transmission code. The algorithm would then add the **R** to its string and checks to see if the dictionary contains an entry that represents **AR**. It does not. The algorithm would then output the codeword that represents the 1-character string "**A**" and create an entry to represent "**AR**". Since the last entry in the initial portion of the codebook is codeword 258, codeword 259 would be assigned to the string "**AR**". Since an output would have been made to represent the "**A**", it would be deleted from the current processing string. The current processing string would then be the single character "**AR**", to which the next character to be transmitted would be added and processing would continue.

(U) The dictionary grows in the form of a tree structure. It might be thought of as a family tree. Except for the immortal root node primogenitors created by the CCIT Gods, every dictionary entry has a parent. The entry "inherits" its parent's string to which is added one additional terminal character.

(U) Once the dictionary reaches its maximum size, the algorithm cycles around to the beginning

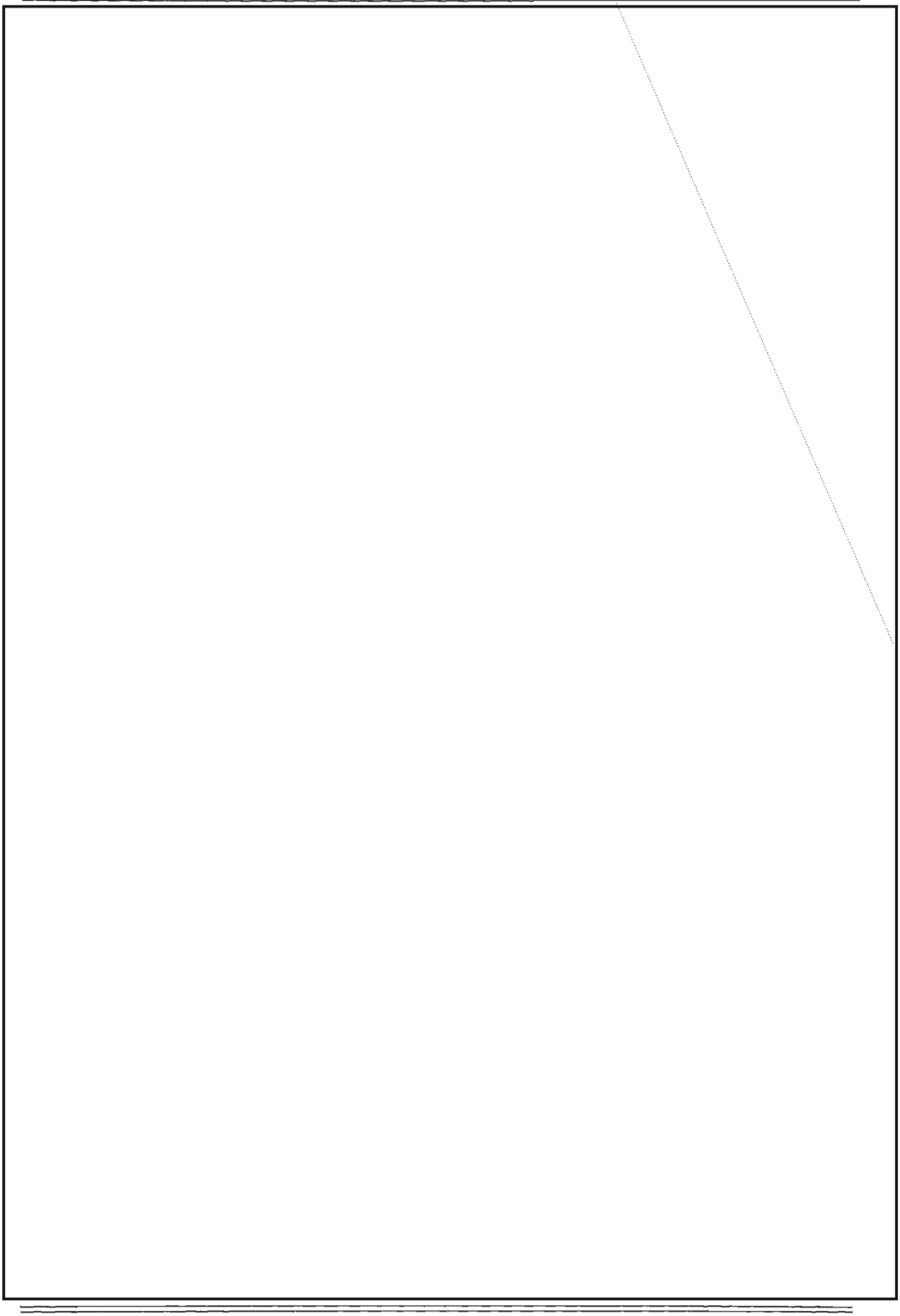
of the non-fixed portion of the dictionary (which starts at codeword 259), and begins searching for "leaf nodes." A "leaf node" is a codeword that has no children, i.e., there is no dictionary entry that represents its string plus one additional character. When a leaf node is found, its string is released and its codeword number is used for the next dictionary entry to be made. (This is a merciless algorithm that tells its creations, "Be fruitful and multiply. If you are barren when next I pass this way, I will zap you!")

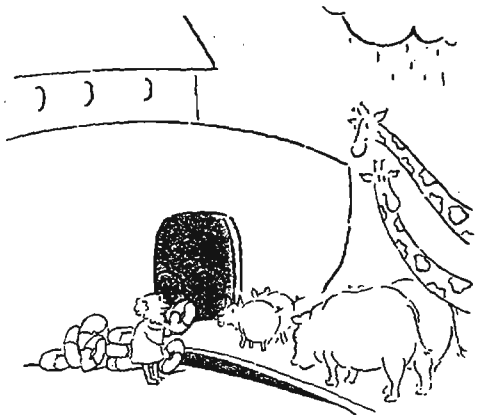
we capture the entries that were made from the point where the cut-in began? We know the process. We know that a dictionary entry was made when codeword 700, the initial codeword of our cut-in, was sent. We know the string to assign to the new entry is the string represented by its parent (700) plus the first character of the string



Each non-root node has a "parent." The "child" represents the "parent's" string plus 1 added character.

(C) For some months, Dr. Ralph Jollensten and I have been developing tools to attack this cut-in problem. Designing the tools has been a cooperative venture. I turn them into software routines and then Ralph has the fun of testing them against simulated cut-ins that I create for him.

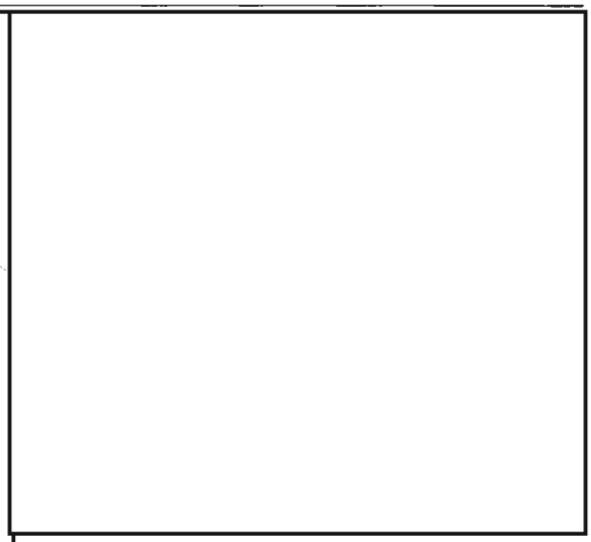




ALL YOU WANTED TO NOAH ABOUT ARC

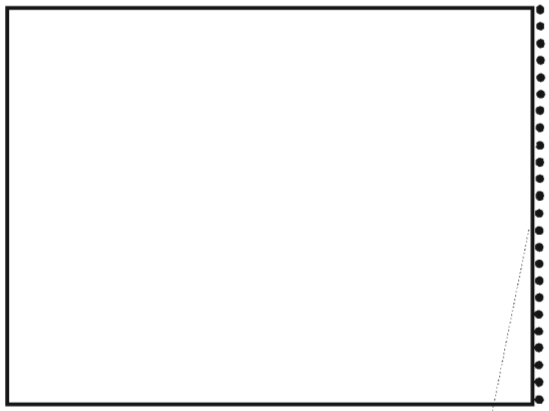
P.L. 86-36

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



ERRATA

In 3rd Issue 1990, several lines were inadvertently omitted between pp. 14 and 15. They should read:



FILTERING AND CHARACTERIZATION

~~(C)~~ Filtering is decision making. Every act within the SIGINT cycle in which items are identified and evaluated for retention or rejection is an act of filtering. The act can be mechanized, or can be performed by humans who make the selection, allocate the sensors for the collection activity, and make other decisions about the SIGINT process.

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

In 3rd Issue 1990, on pp 14-18 and 20, please change the issue to ""3rd Issue 1990"

CRYPTOLOG regrets the errors

~~CONFIDENTIAL~~

CRYSCO-90

~~This article is classified CONFIDENTIAL-HANDLE VIA COMINT CHANNELS ONLY in its entirety~~

The Cryptanalytic Software Committee (CRYSCOM) was established in May 1984 as a volunteer organization to improve the use of computers throughout the entire cryptanalytic community by providing a forum where representatives of the CA computer complexes could exchange ideas. In 1987 it was officially sanctioned when its charter was signed by the Office Chiefs of the major CA complexes at NSA. CRYSCOM provides a formal mechanism for the collection and dissemination of information on computer support [redacted]

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

The Cryptanalytic Software Conference (CRYSCO) is an annual event where current topics on cryptanalysis and computer science are presented. Following are the recommendations stemming from CRYSCO-90.

1. Software Availability

Develop and promote a softcopy method of listing all available software on all appropriate machines in the CRYSCOM community, to include pending software, also to include software which makes use of special purpose boards or devices.

Status: Notesfiles, software.ad and software.quest, were created. Some user organizations are using them, while other organizations are developing their own library functions.

2. Software Exchange

a. Continue efforts to establish and promote software exchanges. [redacted]

b. Encourage organizations to adhere to agreed upon standards.

c. Promote the goal of a man page for every piece of software.

Status: The number of software exchanges is growing and ground level satisfaction with and success using the procedures has encouraged the organizations to adhere to the agreed upon standards. The goal of a man page for every piece of software exchanged has been attained. Feedback through the Software Points of Contact has been perceived as effective.

3. CRYSCOM Character Message Format:

Resolve outstanding disagreement on header line tags.

Status: Parties involved recognize the header line tag issue as a difference to be aware of as opposed to an outstanding disagreement. The committee agreed to table this recommendation.

4. X-Window Widget Sets :

[redacted]

Status: A working group has been formed and is evaluating toolkits.

P.L. 86-36

5. Public Domain Software

a. Look for a method of obtaining public domain software.

b. Establish a procedure to propagate error reports for public domain software back to originators, particularly, X-Windows, Gnu products.

c. Establish a procedure to propagate fixes back to the users.

Status: R5 is setting up a mechanism for evaluating public domain software, which will be available for use by community members. After this evaluation process, CRYSCOM intends to submit a list of specific software to T03 with a request for consideration.

6. System Administrators:

Organize a forum for the various system administrators, especially those of the numerous SUN networks, to discuss mutual concerns, such as security issues, response times, network transparency, etc.

Status: Completed.

7. Training

P.L. 86-36

Lack of UNIX training is seen as a big problem in the move [redacted] Promote UNIX training, such as through brown bag seminars.

Status: Brown Bag seminars will be reinstituted to promote UNIX training and expertise.

8. NQS Checkpointing and Restarting:

Promote the resolution of NQS checkpointing and restarting problems.

Status: A list of capabilities wanted in NQS has been supplied to Cray, who will work to incorporate them in a future release.

9. Software Development Tools

Promote development, acquisition and use of appropriate software development tools; especially optimization tools, graphics aids, timing tools.

Status: CRYSCOM is working with W352 to arrange for a brown bag seminar on optimization. This recommendation is one which will be an ongoing concern.

10. CRYSCOM "Official Papers"

Create a directory/catalog of such papers to include: CRYSCO recommendations, position papers, guidelines, standards, etc. In short, any voted on document.

Status: Completed

To the Editor:

Though there's a lot of expressed concern about "The" language problem and keeping linguists happy, management actions belie that concern. Look where they located the Language Career Panel, for one thing. It's at Friendship. Where are the linguists? At Fort Meade.

Linguists have more in front of them than they can possibly do. For a lot of languages there's a severe shortfall. So why are they compelled to travel to Friendship in connection with career development?

Why does management allow this inane situation to continue?

Why don't the linguists rise up and protest?

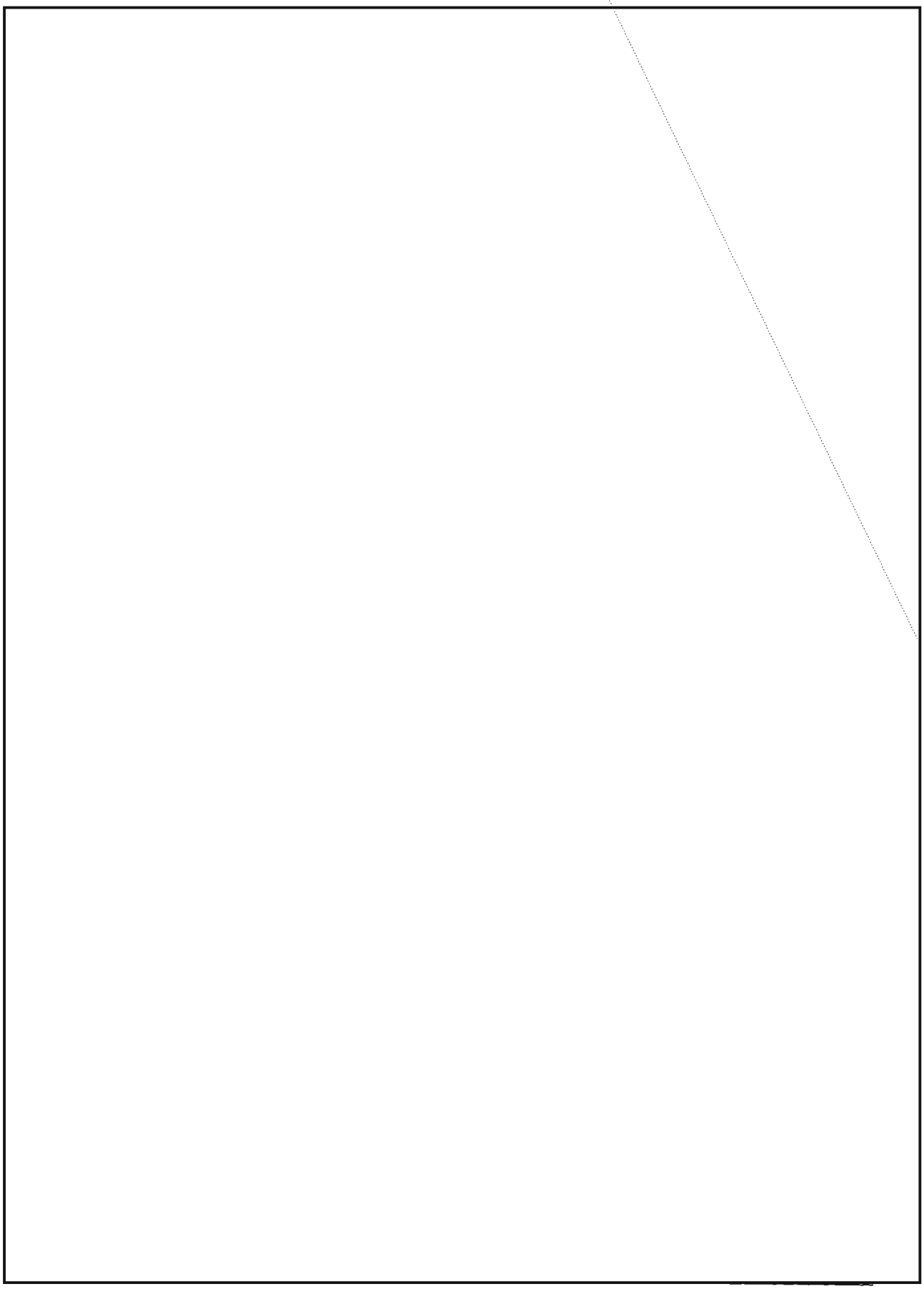
"Al Enquist"

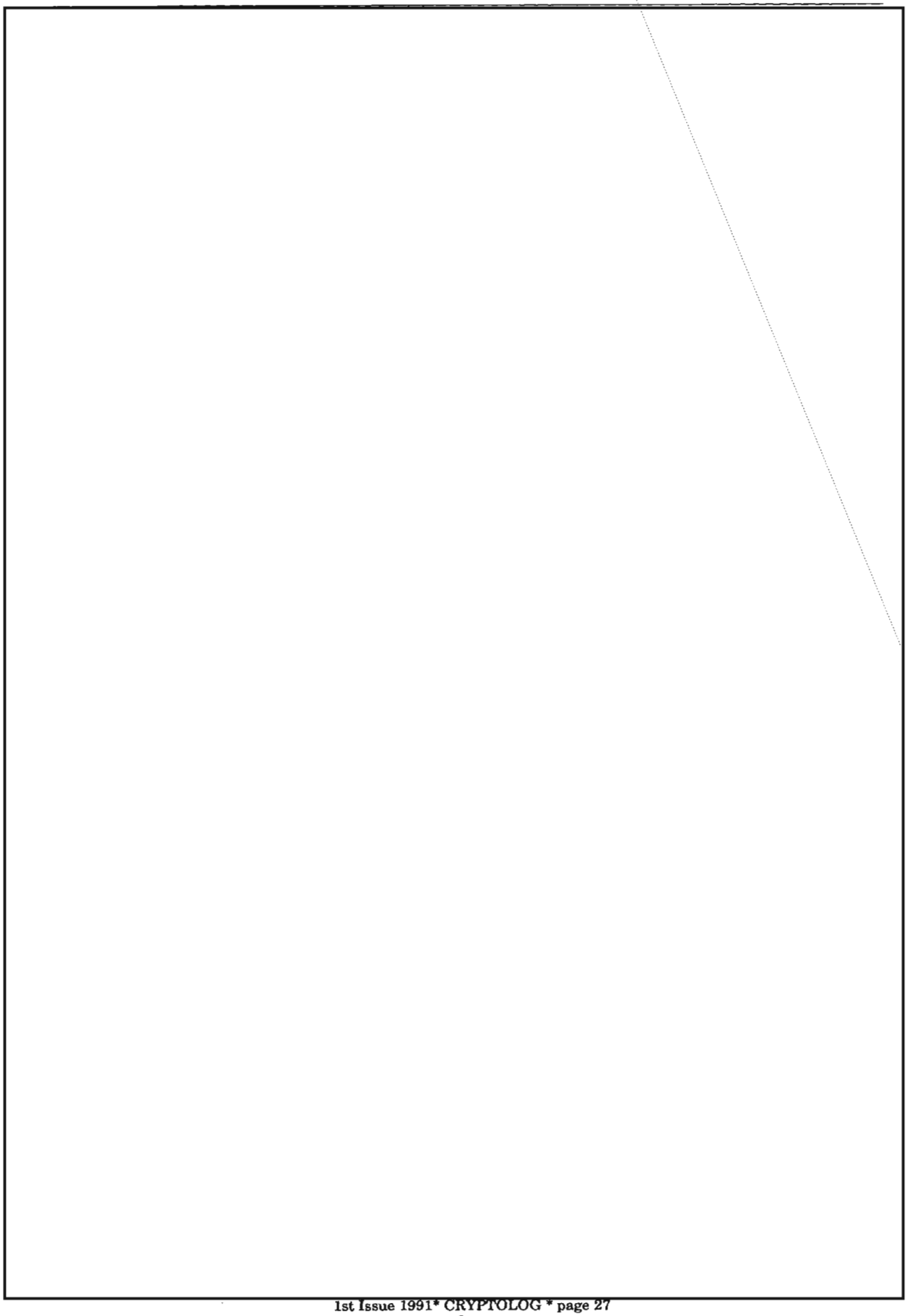
~~FOUO~~

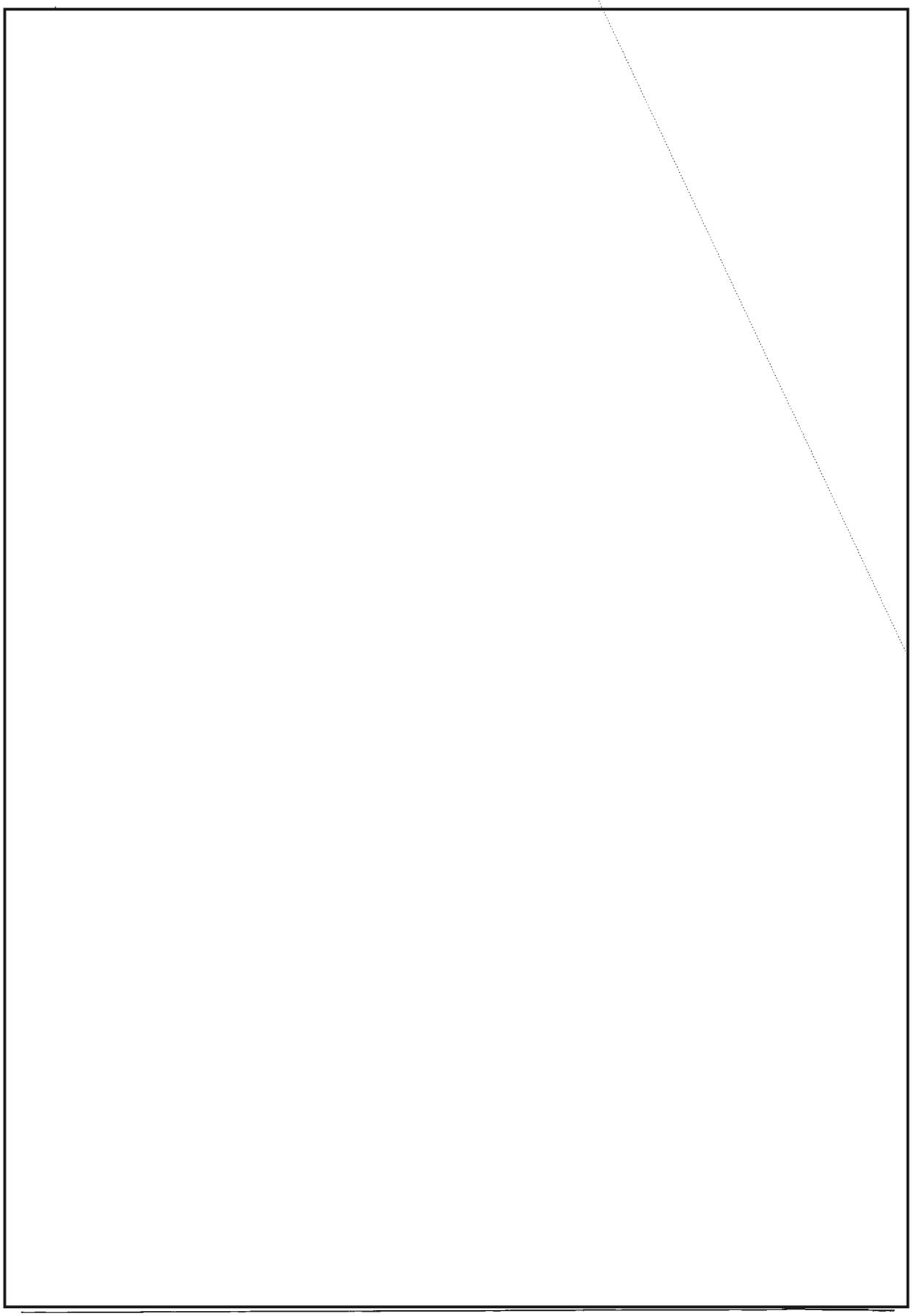
Normalization

P.L. 86-36

[redacted] *A26*







~~CONFIDENTIAL~~

To the Editor:

I read with interest the item by Preston Currier on the subject of Cryptographic Habits and Cryptanalytic Diagnosis, an extract from his 1969 papers [CRYPTOLOG, 3rd Issue 1990].

I thought you be be interested in knowing that T54 (Archives and Repository Services) is attempting to record historic cryptographic information, i.e., codebooks and technical papers for the period pre-1975, in a special electronic database referred to as the "Cryptographic Codes and Ciphers Collection." This information is unique and does not duplicate C/A information in other Agency collections, i.e., P1 Collection, etc.

This endeavor by T54 is quite massive and will require considerable time to complete; however, the initial progress that has been made to date has proven extremely worthwhile and has attracted the interest of many cryptanalysts from various OPIs in the Agency.

I am taking the liberty of forwarding you two recent communications by [redacted] G424/H111 after his research into various T54 treasures and the results of his efforts in support of a current high-interest cryptosystem that he was assigned. I believe you will find these of interest.

Should you wish a follow-up to the [redacted] article, these comments by a young cryptomath analyst may alert other analysts in this discipline to the wealth of information developed by our predecessors and now becoming available in T54, Archives and Repository Services, and D9, NSA Center for Cryptologic History.

[redacted] *T541 Archivist for C/A*

~~CONFIDENTIAL CCO~~

~~SECRET~~

P05/SAO

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

P.L. 86-36

in re PROFORMA

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

P.L. 86-36

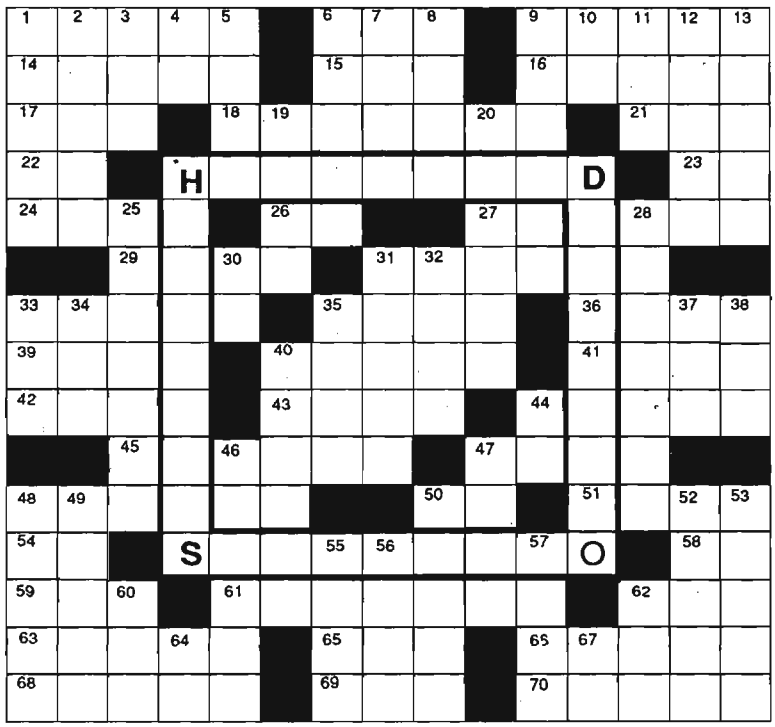
P.L. 86-36

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

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

Busman's Holiday

This puzzle is dedicated to William Lutwiniak, the founding publisher of CRYPTOLOG, himself a noted puzzle-maker, to mark a half-century's association with cryptology. *See page 7.*



ACROSS

1. '50's chewing gum favorite
6. Word with fly and about
9. *Enterprise*- ing mate
14. Seen less often
15. Basketball great(?) Blab
16. Give a full 10%
17. Wilder pronoun
18. *Odd assortment*
21. Oldie but goodie "___ Then"
22. Correlative alternative to 60-D

*** CLOCKWISE**

23. Generic Mrs./Miss
24. Marx missing from *Monkey Business*
26. "___ you is or ain't you ain't . . ."
27. Syria's second-largest city
29. Now-stout Guinness
31. Entertaining Lola
33. Washington August forecast
35. Guitar-wielding Hendrix
36. *Imperial contents*
39. Man from Medina
40. Donny's little sister
41. "A ___ by any other name . . ."
42. Hero Jones at the 500?
43. The class of Hitchcock's creatures?
44. Thomas or Bob
45. *Detroit's Joe Louis and Baltimore's Baltimore*
47. Pull a long face
48. Place name in the '60's news
50. Cerium's symbol
51. ___ off, angry à la Curtis Strange
54. A's pre-vowel substitute
58. Behold's partner
59. Anais
61. Settle the details
62. Coulomb per sec.
63. Imperturbable one
65. Explosive stuff
66. Plains home
68. Down to ___
69. Opp. of WNW
70. Angel-owning cowboy crooner

DOWN

1. Flashback: your President is not one
2. A Dern-good actress?
3. Hockey great
4. Fine day in 1945
5. Bombeck
6. Drinks in air
7. Far and ___
8. Xiaoping
9. Brando cry in *Desire*
10. ___ are not ^{2}
11. Baseball great
12. Bonzo, for one
13. Horse racing great
19. *The Iliad* or *The Odyssey*
20. Netminder
25. Fast month in 27-A
28. One who has done his time—partially
30. Wilbur Post's pet
31. Bakes pottery
32. Kingsley
33. "Bali ___"
34. Coffee maker
35. Contents of above, in Indonesia?
37. ___ a matter of fact
38. Another Kingsley
40. Crèche component
44. Ti's successor
46. Fortify bread
47. *La carte*
48. Saint-Saens ___ *Macabre*
49. Baker who's "Giving You the Best That I Got"
50. $100
52. Siwwy Wabbit's foe
53. One of Doc's little buddies
55. Participate on the 2nd Tues. in Nov.
56. Holiday and Days
57. ___ boy!
60. See 22-A
62. Likely to be good at?
64. Stephen King's ___
67. Prefix opp. to *dys-*

RLW

Editorial

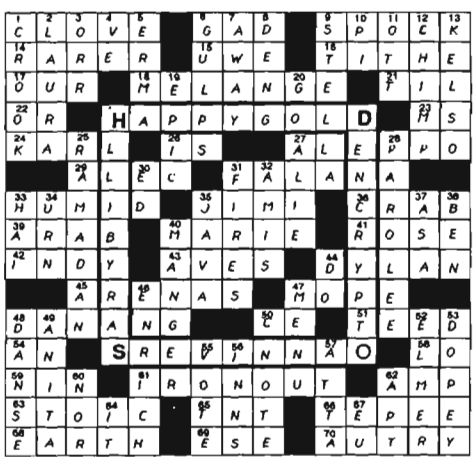
Lessons Learned

With a certain amount of euphoria, some veterans of past crises were commenting on the most recent one in which they were but spectators. They were pleased with the high interest in "lessons learned." It's important to record and act upon these, they believe, and the record should include the minutest detail of things gone wrong. The causes of serious problems can often be traced to the snowballing effect of many minor errors that were disregarded.

From their distant perch, these veterans noticed the beginnings of changes in some of the operational elements that were not directly involved in the crisis but that contributed people and material resources. Somehow those elements found ways to function more efficiently with fewer people. Maybe they, too, should be included in a "lessons learned." In a leaner operation, there was no time to pay tribute to arbitrary prerogatives. Surely the newly streamlined mode deserves close study, and perhaps, emulation elsewhere.

Va

Solution to Puzzle on page 31



BULLETIN BOARD

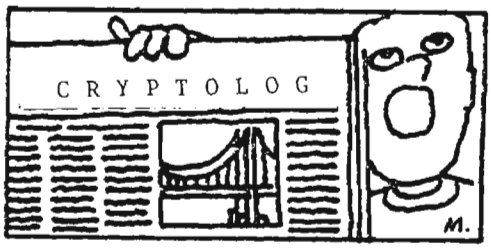
RECOVERING DELETED DATA ON THE SUN

~~(FOUO)~~ R522 found a way to recover deleted data on the SUN. A typing mistake had resulted in the deletion of an entire directory of files dealing with the TANCIL software. The SUN people and other experts estimated that the chances of recovery ranged from poor to none.

~~(FOUO)~~ But R522 experimented with a method that proved to be successful in recovering files, especially source code. All you have to do is lock the file system long enough to make a copy to work with offline. Using this technique, R522 was able to recover most of the TANCIL software. For more information call [redacted] R522, 968-8411.

P.L. 86-36

Notice to Subscribers



Distribution for this issue reflects changes received by COB 13 May 1991.

If you move or are reorganized, please notify CRYPTOLOG DISTRIBUTION, P1, NORTH. Be sure to indicate both your old **and** new organization and building.

CRYPTOLOG

Editorial Policy

CRYPTOLOG is a forum for the informal exchange of information by the analytic workforce. Criteria for publication are: that in the opinion of the reviewers, readers will find the article useful or interesting; that the facts are accurate; that the terminology is correct and appropriate to the discipline. Articles may be classified up to and including TSC.

Technical articles are preferred over non-technical; classified over unclassified; shorter articles over longer.

Comments and letters are solicited. We invite readers to contribute conference reports and reviews of books, articles, software and hardware that pertain to our mission or to any of our disciplines. Humor is welcome, too.

If you are a new author, please request "Guidelines for CRYPTOLOG Authors."

How to Submit your Article

Back in the days when CRYPTOLOG was prepared on the then state-of-the-art, a Selectric typewriter, an article might be dashed off on the back of a used lunch bag. But now we're into automation. We appreciate it when authors are, too.

> *N.B.* If the following instructions are a mystery to you, please call upon your local ADP support for enlightenment. As each organization has its own policies and as there's a myriad of terminals out there, CRYPTOLOG regrets that it cannot advise you.

Send two legible hard copies accompanied by a floppy, disk, or cartridge as described below, or use electronic mail. In your electronic medium (floppy, disk, cartridge, or electronic mail) please heed these strictures to avoid extra data prep that will delay publication:

- do not type your article in capital letters
- do not right-justify
- do not double space between lines
- but **do** double space between paragraphs
- do not indent for a new paragraph
- but **do** paragraph classify
- do not format an HD as DD or vice-versa–our equipment can't cope

The electronic mail address is *via* PLATFORM: cryptlg @ barlc05
or *via* CLOVER: cryptlg @ bloomfield

CRYPTOLOG publishes using Macintosh and Xerox Star. It can read output from the equipment shown below. If you have something else, check with the editor, as new conversions are being added. Be sure to label your floppy or cartridge as to the hardware, density, format, and software you used. Don't forget your name, building, organization, and phone!

HARDWARE	MEDIUM	SOFTWARE	FORMAT
SUN	60 or 150 MB cartridge	ascii only	TAR or RAW
XEROX VP 2.0	5 1/4" floppy only	n/a	n/a
MACINTOSH	3 1/2" DD disk only	MS WORD MacWrite TEXT WriteNow	n/a
IBM & Compatibles	3 1/2" 1.2 MB disk 5 1/4" DD or HD floppy	MS WORD WordPerfect WordStar ascii DCA (IBM revisable)	DOS
WANG	n/a	n/a	n/a

~~TOP SECRET~~