~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JUNE 1978

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

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

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

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

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. V, NO. 6 JUNE 1978

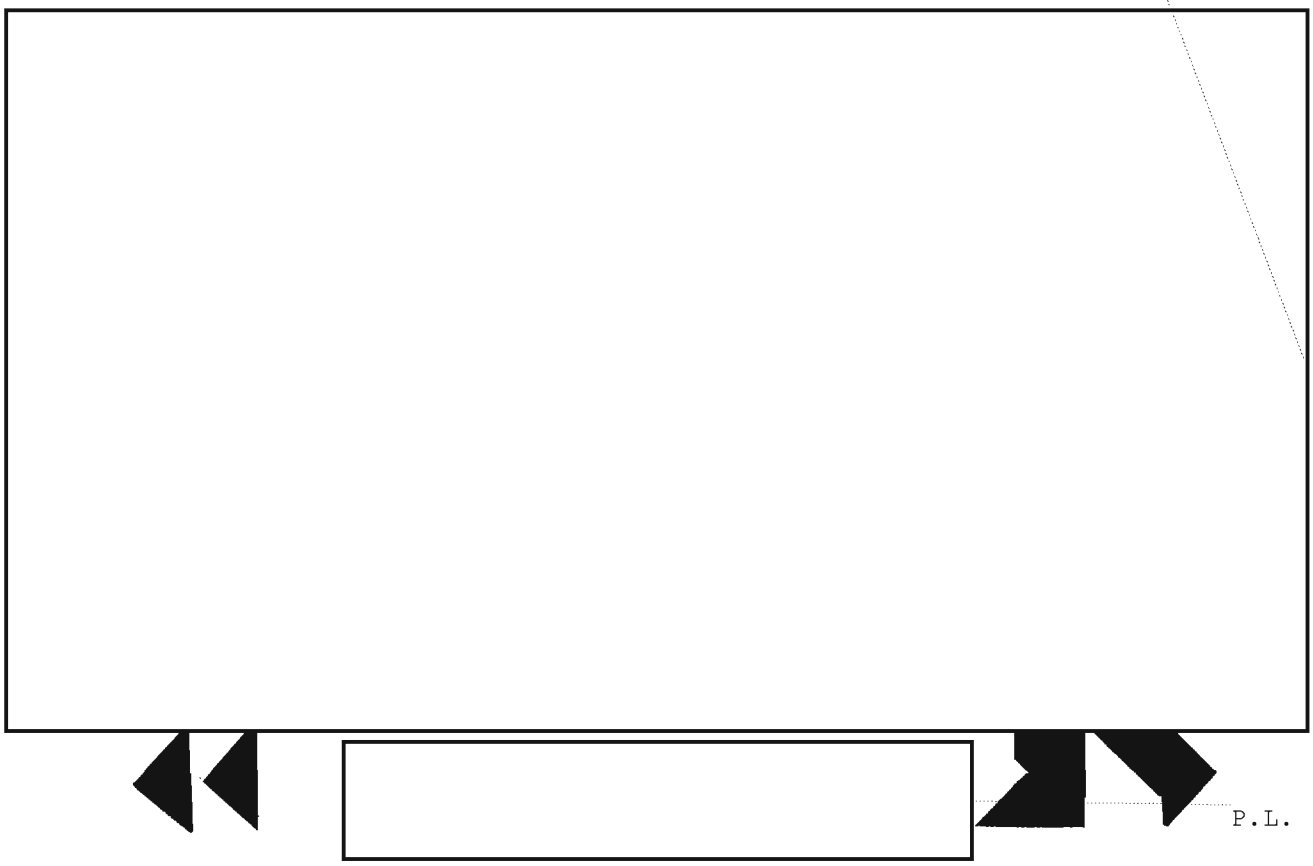
PUBLISHER WILLIAM LUTWINIAK

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

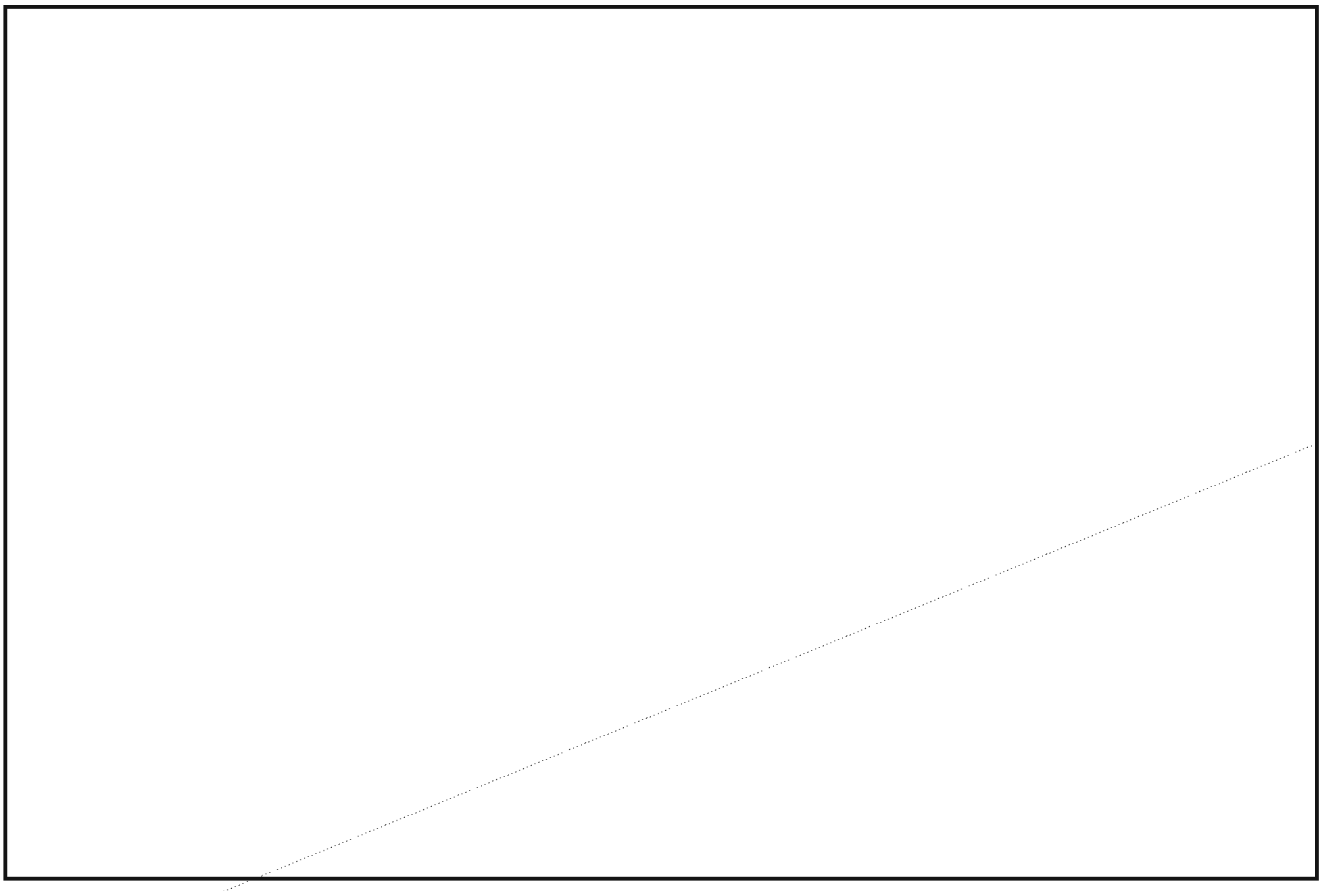
~~TOP SECRET~~

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

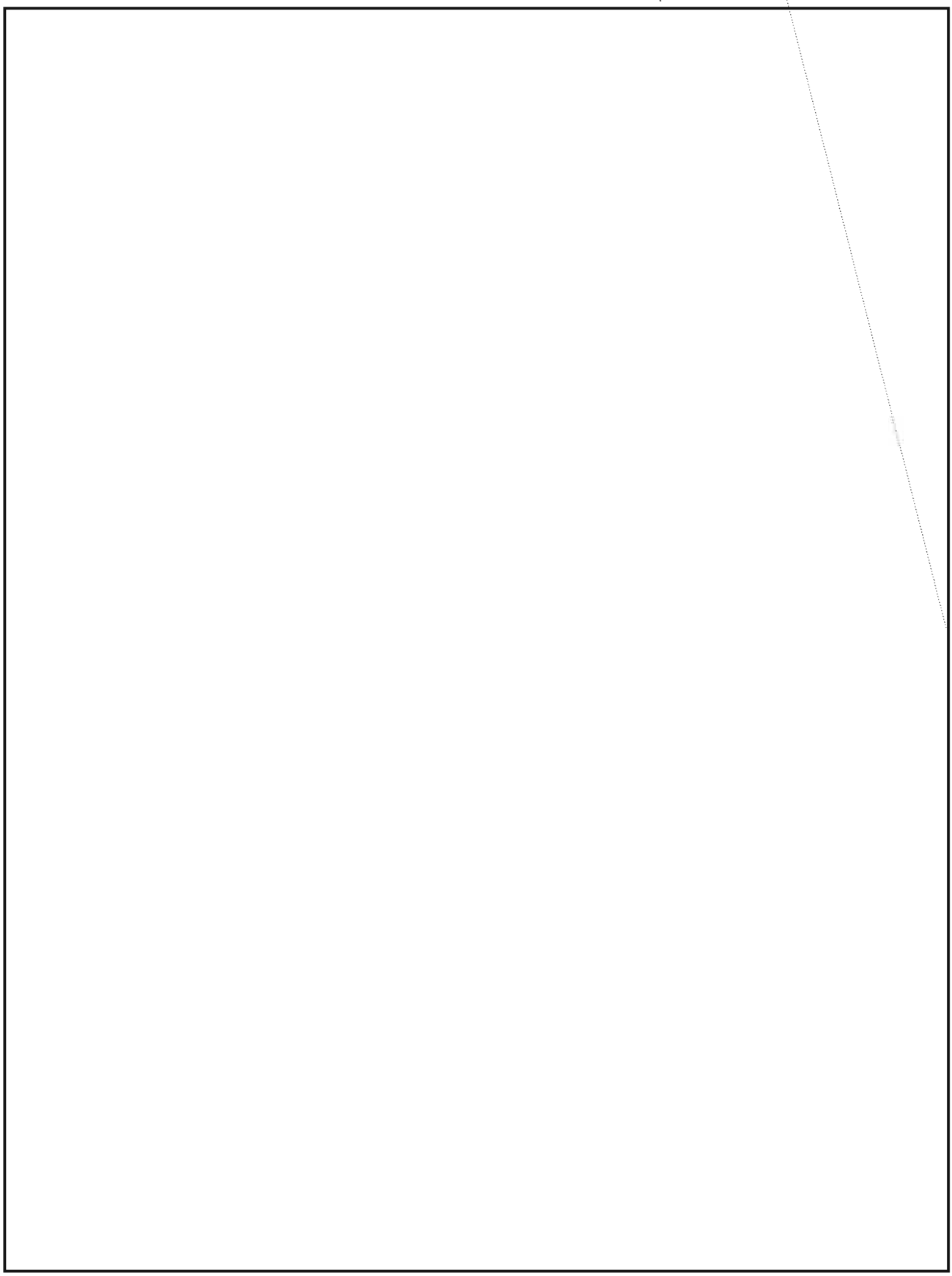
~~TOP SECRET UMBRA~~

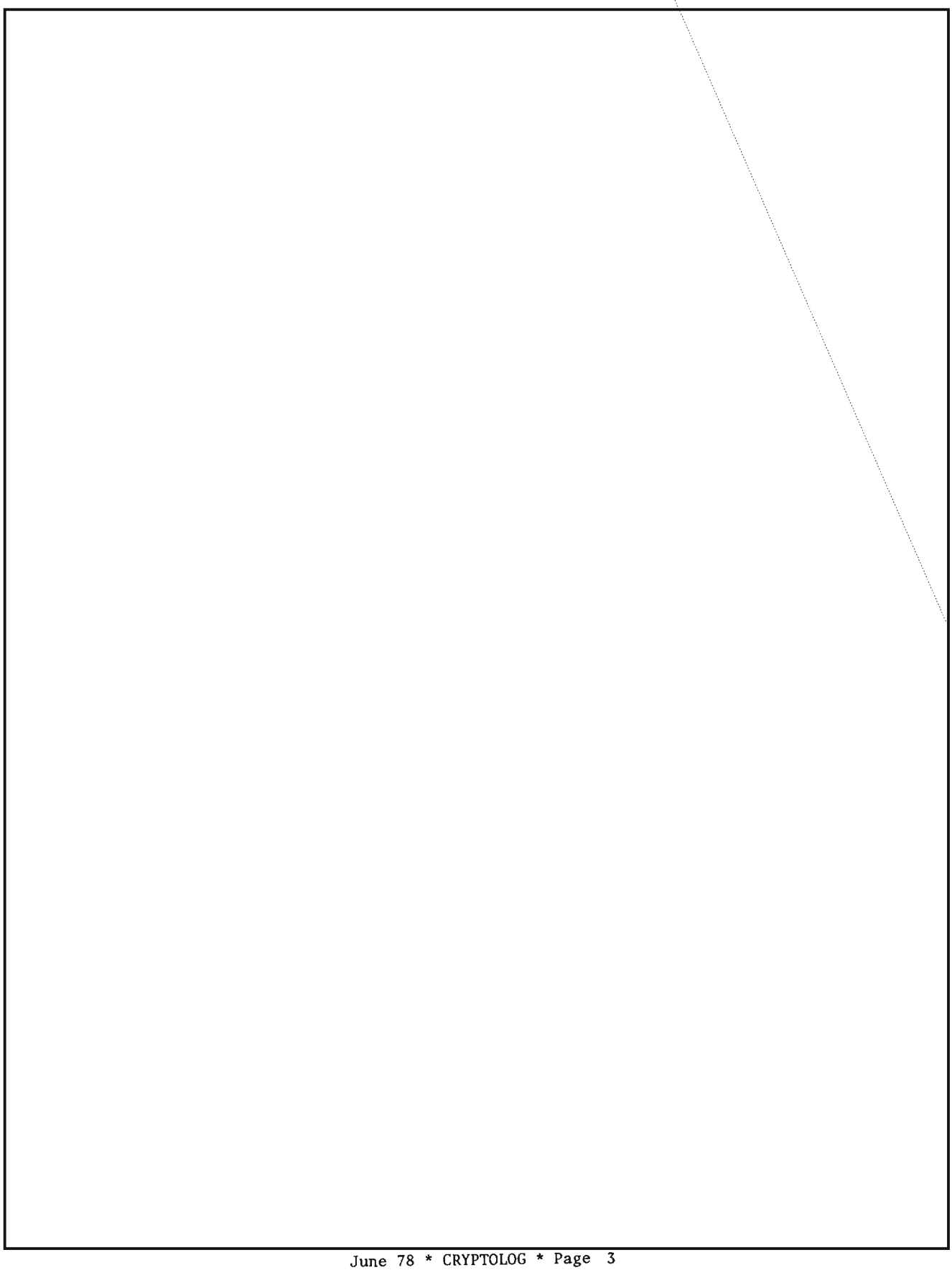


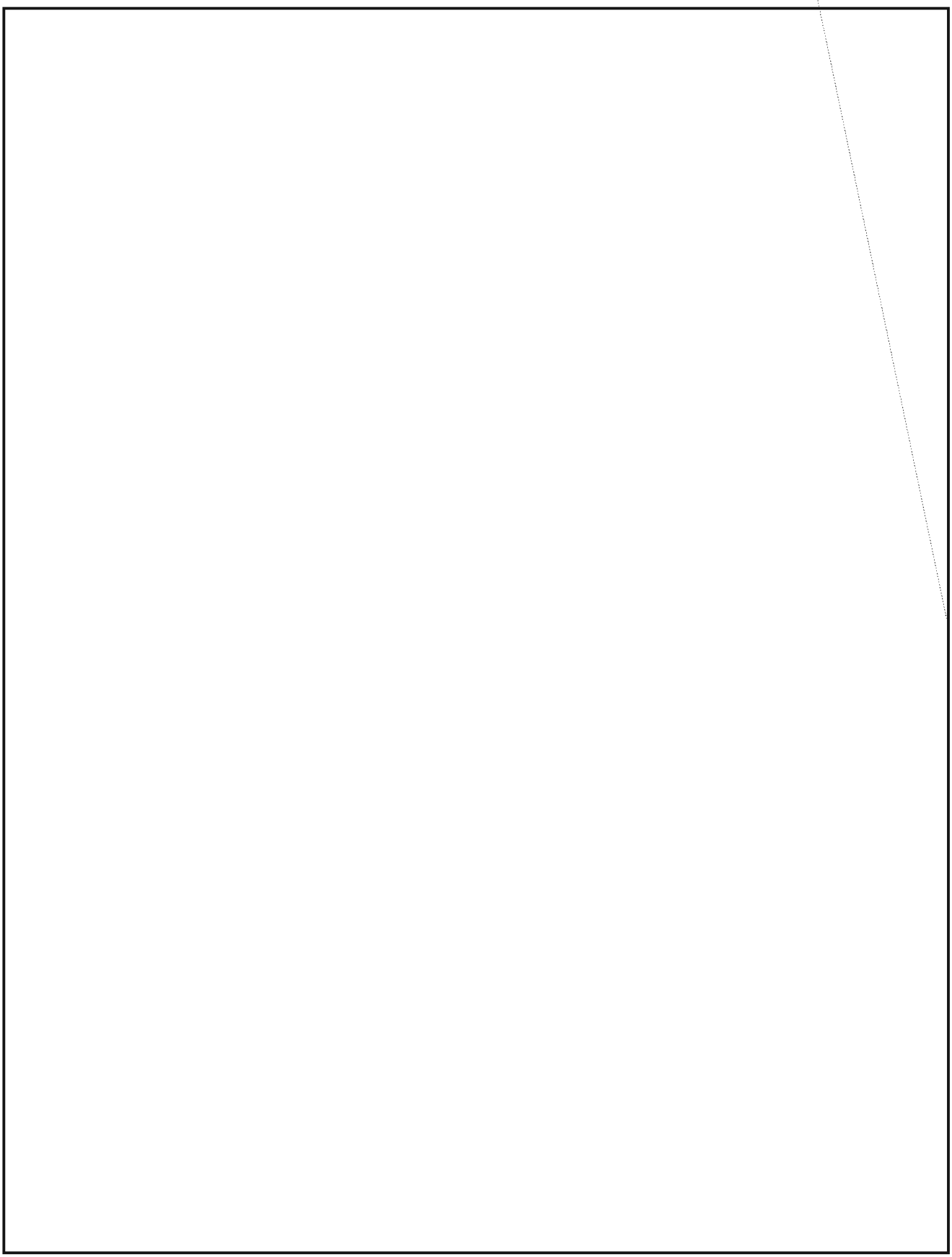
P.L. 86-36

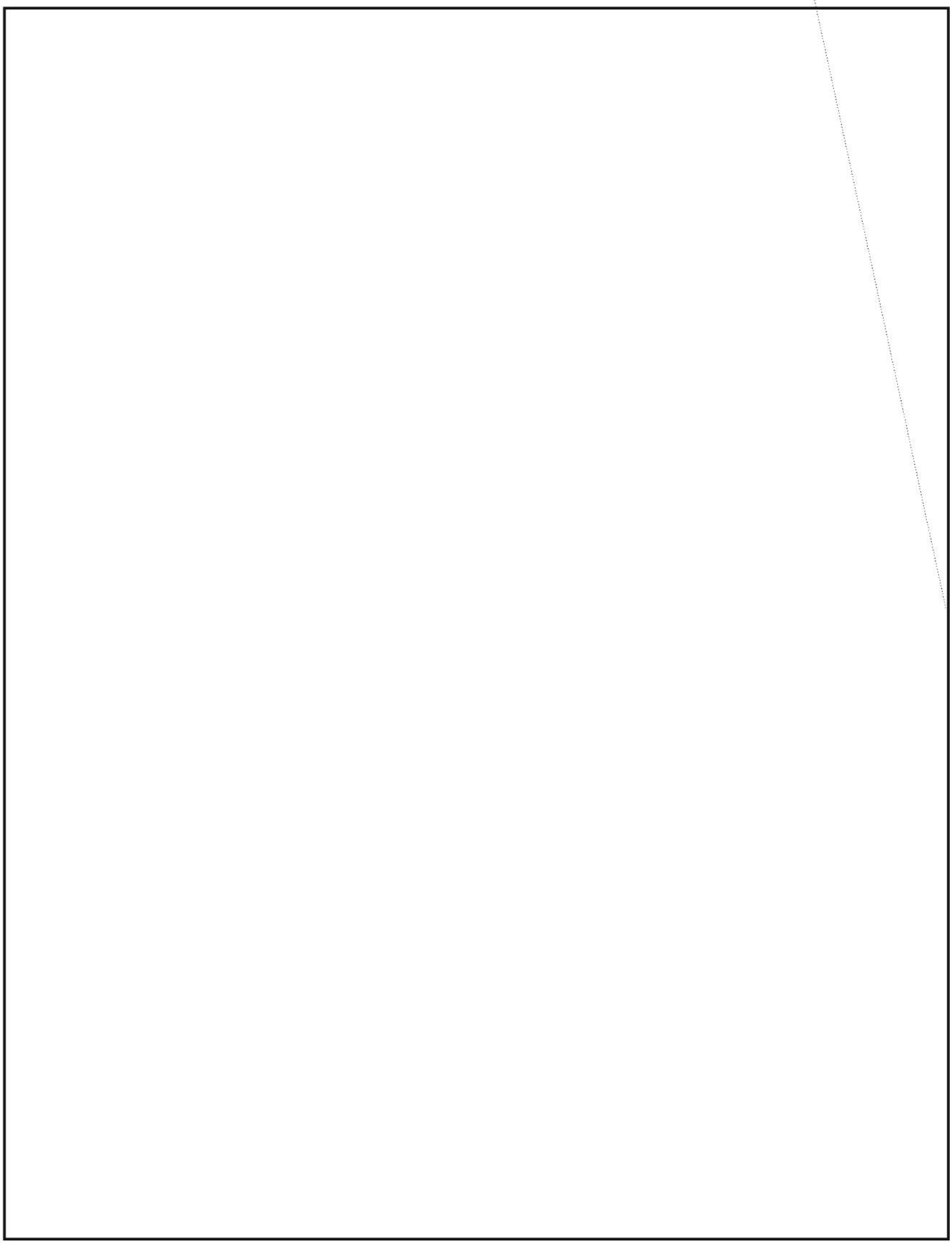


EO 1.4.(c)
P.L. 86-36









[redacted]

~~(TSC)~~

BOOKBREAKERS FORUM ON MACHINE AIDS

Do you know...

...that the Bookbreakers Forum is currently developing a new set of bookbreaking runs?

In the 10 years since the present Bookbreakers Package was designed, there have been remarkable advances in computer technology.

[redacted]

If you have any ideas that you would like to see incorporated in the new set of bookbreaking runs being developed, get in touch with: Bookbreakers Forum, [redacted] Chairman, P16, 5642s, Room 2N039.

~~(C CCO)~~

Solution to NSA-crostic No. 14

by "Sardonyx" (CRYPTOLOG, May 1978)

[redacted] "Freedom in Translation," *NSA Technical Journal*, Vol. XXI, No. 3, Summer 1976:

"Testing and checking always seem to create a climate where conservative attitudes prevail. Setting standards in anything, by its very nature, focuses on the minimum which is required to do the job rather than on excellence of performance."

(U)

EQUIPMENT MAINTENANCE ON ABNER

[redacted] D/Chief, R7

The article by [redacted] in the August 1977 CRYPTOLOG provided an excellent perspective of how the programmers viewed ABNER. [redacted] followup letter in the November 1977 CRYPTOLOG provided additional insights on the construction of the equipment. I believe it would be remiss not to cover at least a few points concerning some aspects of the equipment maintenance on the ABNER Serial 1 system.

When AFSA, NSA's predecessor at Arlington Hall Station, first determined in the very early 1950s that it was getting into the electronic computer arena, it was readily determined that there was no source of qualified engineering or electronic computer-maintenance personnel to be enticed into service at the Agency. In addition to hiring a few civilian electronic engineers and technicians, it was decided to attempt to get some expertise in this area by seeking military officers. A survey indicated that the training that came closest to meeting the Agency's requirements was given at the Ground Electronics (Radar) School at Keesler Air Force Base. A levy was placed on the USAF/AFSA for one officer in the top third of each of ten succeeding graduating classes. I was "fortunate" enough to be selected as the first officer from the first class. Upon arrival at Arlington Hall, I was assigned to the computer maintenance for ABNER. People like [redacted] now Chief T2 (as well as [redacted] all of whom are still at NSA), were old hands at ABNER maintenance, having already spent about 6 months working side by side with the development engineers and programmers in anticipation of the computer's becoming operational.

ABNER I, Serial 1, the first NSA application of "serial dynamic logic" circuitry, presented new problems for isolating malfunctions. The computer, including the consoles and peripherals, came close to being a maintenance nightmare. All of the electronic D.C. power supplies were of the laboratory type, with variable voltages. They were not overly stable and they generated a tremendous amount of heat. Electrosonic mercury delay lines were used for the 1024 words of memory (512 words per cabinet, or 64 delay lines per cabinet). The only pluggable components in the whole machine were the diode/resistor gates (there were 25,000 1N34 diodes) and the 6AN5 vacuum tubes that were used for digital pulse amplifiers. There were about 1500 6AN5s, all being used close to their design rating, and they had an MTBF that did not endear them to the maintenance personnel. More importantly, all the digital pulses were processed through various lengths of electronic delay lines. The latter were all wire-bound on very delicate metallic-plated fiberglass rods and hard-wired into the system. Likewise, all the pulse transformers were hard-wired into the system and when we were so fortunate as to locate a faulty delay line, pulse transformer, or diode isolating/gating circuitry, it took at least a half-hour or more to replace the suspect component if it was not a tube or a plug-in gate.

Perhaps more important than the hardware replacement problem was the fact that there were almost no electrical or software diagnostics for the machine. The R&D programmers had developed a few "exercise" routines, but the usual "maintenance" technique was to attempt to run an operational program and, when it didn't work, Maintenance was called in to see if we could find the trouble. This was the standard practice in other "computer laboratories" in the United States during this early computer era. Over a period of time, of course, we did develop some diagnostics. Many problems, however, occurred with the electromechanical input and output equipment and with the operations console itself. These faults would, of course, bring everything to a grinding halt, since then we could not even get data into or out of the machine. We were also hampered because the response time of the oscilloscopes was so slow that it was difficult to "see" some of the pulse trains, and delayed-sweep oscilloscopes were not yet in use.

P.L. 86-36

When production operations started in 1952 there was no time allocated for preventive maintenance. All the maintenance time we were allowed was that necessary to correct faults. In general the machine was used during the day shift by the R&D personnel who were continuing to develop some facets of the equipment and, in some cases, to improve reliability.* During the evening shifts it was used by the programmers who were just developing some of the initial programs [redacted] was among the best of these) and the attempt was made during the midnight shift to run on an operational basis the few programs that worked. All three of these "customers" (the R&D engineers and programmers; the operational programmers; and the operators) provided a unique technical as well as human-relations challenge to the maintenance crew.

As time went on, things of course improved. The maintenance people still thought the

equipment was poorly designed; the programmers were probably the happiest of the lot; the R&D engineers were glad to get on to newer things; and the operations people suffered through with all of us. As Art Salemme wrote in the October 1977 *NSA Newsletter*, most of us lived in the Buckingham area and it was not uncommon to work on the machine for several hours at a time, come home and get something to eat (with logic equations and microseconds still going through our brains), and wander back down to work to see if we could try one more idea in the attempt to fix the machine. Maintenance down times of 4 to 8 hours were very common and on occasions lasted up to 4 or 5 days. This was not so much a reflection on the quality of maintenance personnel (I would like to think), as a reflection of the complexity of the design, the newness of the whole concept, and the absence of statistically reliable preventive maintenance procedures and software diagnostics. In many cases, whenever we were sure the input and output equipment and console were working, we would write down our own diagnostics to try and locate a sticky logic problem in the machine. As each new computer application program was written, it was not uncommon to find logic errors in either concept or wiring, even after the first year or two of operation.

After approximately a year of such interesting endeavors, I was considered qualified to become the maintenance chief on a special-purpose machine, DELLA, being constructed by R&D using the same type of digital logic and components (albeit with many more plug-in components used), that was expected to come into operations. DELLA was to be located at Nebraska Avenue and I soon began the joys of carpooling from Arlington to NSS and lost contact with ABNER just as it came into its own as a highly productive piece of computing/analytical equipment.

~~(FOUO)~~

DEPARTMENT OF GOLDEN OLDIES

EXISTENCE OF UNIDENTIFIED UNIT TENTATIVELY ASSUMED AT UNKNOWN LOCATION

One of our regular contributors recently came across the following item in his files. It was written immediately after some directive came down about not publishing anything that sounded like a snap judgement. It was circulated widely at Arlington Hall Station (see the reference to the originating sub[13]element within AFSA-242) and originally bore the fake classification "Top Secret Blurb."

Ed.

U/I Unit, possibly behind "Iron Curtain"[6]

AFSA-242c3b5d4j7s45x(Ø)[7]
(date garbled)
(X groups missing)

Traffic analysis evidence of a very tenuous nature faintly suggests the remote possibility that an unidentified unit, of undetermined echelon or type, may, in some manner, exist somewhere within Soviet Russia, or in that general vicinity.

The tentative existence of this headquarters, possibly a unit of undetermined echelon or type, is suggested by what is believed to be

5 - Intercept date garbled.

6 - Meaning not clear.

7 - Unlocated.

~~(C - CCO)~~

NEVER AGAIN!

JACK GURIN, R5

I'm not easily angered, and on those occasions when my face reddens and my hands tremble with the realization that something stupid, ridiculous, and unfair has occurred, I cool off rather quickly. But something happened more than a year ago, and even now, whenever I think of it, my face gets flushed and I find myself searching out appropriate epithets (to mutter to myself, of course).

You see, I believed in the system. I trusted it, even though I knew that many around me, although good and loyal members of the establishment, smiled condescendingly when I claimed that it was better to obey the letter and spirit of the regulations than to ignore them. Their condescension clearly conveyed the notion that they were too canny, too experienced in the ways of bureaucracy, to be taken in. A few came out and said that what I proposed to do was a mistake and that I would rue the day. Others merely shrugged their shoulders and said pityingly, "You'll see."

I had a file of papers, the only one of its kind, relating to an experiment which had been conducted in an attempt to improve our processing techniques. Without debating the merits of the original idea or of the experiment itself, which involved not only NSA, but ASA and AFSS as well, let me state that a lot of hard work went into it. After several years of research, training courses, TDY trips, field trials, and interagency correspondence, it was decided to call the experiment off. The records ended up in my safekeeping, and I felt certain that at some time in the future the issue would be revived.

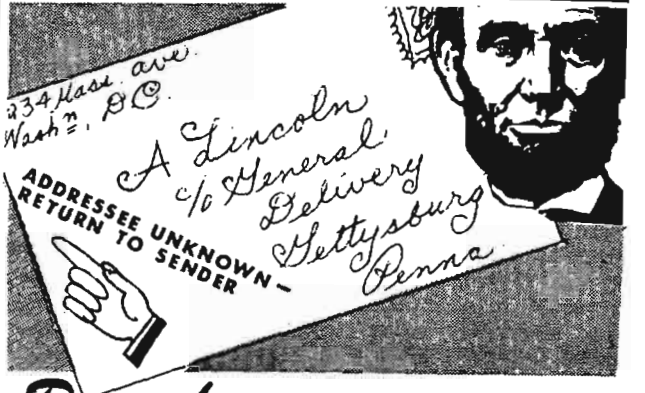
I have always been aware of the heavy cost of filing cabinets and floor space, and I agreed that, if a safe alternative existed, I should not use files in my office to store this material. Besides, I might not be around when the files would be needed again. So I followed the rules and, in September 1967, entrusted the files to NSA's Archives, after carefully noting the contents, and marked them for "Indefinite Retention." I made certain that I had the receipt, which gave the accession number and even the box or shelf number at the storage location. I was *assured* that I could retrieve the file when it would be needed.

Almost 10 years later, in April 1977 (you've already guessed, I'm sure), the subject did come up again, at high levels both within and outside the Agency, and so I proudly pulled out my receipt and called for the file. To my horror, I find that *the entire file has been destroyed!* It seems that "management" became concerned about the amount of material being kept in Indefinite Retention, and in 1971 (while I serving an overseas assignment) a group was charged with examining all the files, discarding any which seemed to have no further value. But nobody had the courtesy (or the courage) to ask me whether the file was worth retaining, even though my name was associated with it. Or maybe it was because it was too much trouble to get in touch with me.

Unable to restore all the data that had been destroyed, I could at least register my rage and warn fellow NSA-ers, so I wrote a letter to "Action Line," in the *NSA Newsletter*. That letter was almost word-for-word what I have described to this point. The "Action Line" editor sent it to the appropriate operational area in the Agency for response, and, when that response proved to be, essentially, "It didn't happen on *my* watch!", my letter was returned to me as inappropriate for publication in "Action Line" (I'll admit it doesn't deal with parking spaces or with people who smoke in no-smoking areas).

But I *do* want to register my rage and warn my fellow NSA-ers. And I still am mad, a year after learning that the material was destroyed. I've learned my lesson: Never again, do you hear, never again, will I trust the system to keep something for me, despite any assurances that the material will be found and returned "in a day or two." And, dear reader, if you have anything stored in archives, you would be wise to check right now to see whether it is still there or has been destroyed.

(U)



Do we have your correct address?

If not, please send the correct one to: CRYPTOLOG, P1.

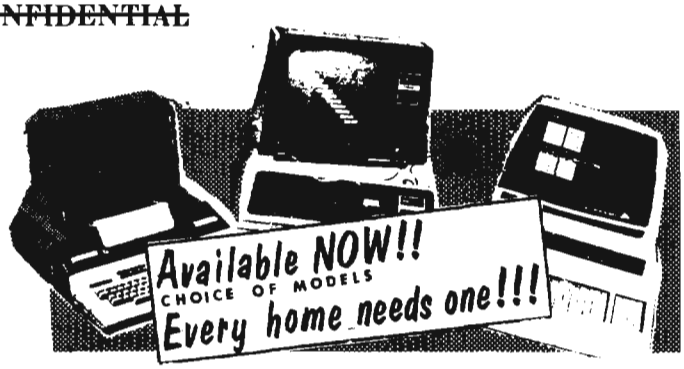
A piece of paper with information such as the following will suffice:

Label reads		Should read
B43		T123

(U)

WHICH WILL WE SEE FIRST...

A COMPUTER SCRATCH PAD AT HOME OR AT WORK?



BILL CROWELL, A204

Something caught my eye in the March issue of CRYPTOLOG. It was [redacted] article "The Hand Is Not Quicker Than the Eye." What Wayne describes is a dilemma shared by a large number of analysts not only at NSA, but also in businesses and in other government agencies: "How can we best use computers to support the human part of the analytic process?" All of us are familiar with the vast capabilities of big computers to crunch numbers, sort data, and print mountains of listings, but do these approaches really support the "personal" aspects of the human analytic process? The type of analysis that Wayne describes involves *insight* into a problem. The type of analysis best solved by the computer support we currently have is the algorithm, a finite solution based on human insight. Essentially, all of the solutions now on computer are the result of off-line analytic processes that are largely unsupported by computer.

Don't get me wrong! Computers *do* support the analyst. They give him data to work on, and they can be programmed to give him that data in myriad ways, including many of the ways that [redacted] described. But I contend that most of the truly analytic processes go unsupported by our computer complex.

Why? Well, there are at least two contributing factors. One was touched on by Wayne: "... we gain analytic insight by doing it ourselves. Logging brings us in contact -- a kind of slow motion contact -- with the material we are studying." His article attests to the fact that, with our current computer support approaches, *contact is lost*. The other fact is that *analysis* is an iterative heuristic process -- trying solutions or parts of solutions until you find one that works or almost works, and then applying those learned lessons in adaptive iteration until a solution is found. Computers are not easily programmed to do this kind of work -- at least not yet. In most cases today, the analyst not only must be able to do analysis but he must also be able to describe to a programmer the process or analysis or ways of achieving *insight* if he wants computer support for his analytic needs. It is difficult enough to do this for his *data* requirements and get what he wants -- and describing data ought to be a hell-of-a-sight easier than describing an analytic process. This is no slap at the programmer -- or at the analyst. If anything, it is just recognition of the limitations of language as a means of conveying quickly a complex analytic process that may have many blind alleys.

P.L. 86-36

Is there a solution to this dilemma? I believe there is, at least to the specific questions that Wayne raised, and perhaps to facilitating all types of analysis. The solution I suggest is not a panacea nor is it new, but perhaps its time has finally come.

The Analyst's Scratch Pad

Almost unnoticed at NSA, the outside world has undergone a revolution in their approach to computer support. The day of the microcomputer has arrived. Not only have thousands of very small businesses begun using them, but -- heaven forbid -- even individuals are buying them, using them, and rapidly creating new applications on them. Oh, you say, these are all engineers and data systems people who want to take their work home with them as a hobby? Not so! None of the people I know who already have a personal computer or have ordered one is an engineer or a data systems professional. One of them is 72 years old and never programmed before -- he is creating a program to analyze the genetics of his cattle herd, and he doesn't think it's too late to learn to use computers.

Why is this happening? There are probably numerous reasons, among them the fact that very capable computers are becoming available at low cost (less than $800). But another reason relates to the desire expressed by Wayne -- to have *contact* with the material they are studying. These new computerists are really analysts who have discovered a powerful new scratch pad for their analytic wanderings. Their ranks are swelling at an incredible rate. So is the product of their labor.

Can any of this analytic-scratch-pad technology be applied to the problem described in Wayne's article? You bet it can! Computerists have found that the instantaneous nature of the computer can be very inhibiting to human beings -- so they created timing loops that simulate human response. They found that endless listings of data befuddled humans -- so they created graphic presentations of the same data so that visual processes can be applied to problems. They encountered problems in handling mistakes made in coding programs -- and created text and word processors to allow the easy manipulation of such data, much in the manner than a callsign analyst would love to be able to do.

Does NSA plan to provide such a capability to their analysts? No! At least not soon and perhaps not until most NSA analysts have a more useful capability at home than they have at work. This is one case where the bureaucratic process has developed a life cycle that far exceeds the cycle of development of new systems and capabilities and costs outside NSA. The budget for FY-80 is being built now and it will have us buying more of the large computer systems available last year or the year before. There is money for collection and for processing, but not for analytic support -- at least not the type of support Wayne and other analysts want!

Emotional response? Yes, it is emotional, but only because I think NSA is missing an opportunity. We have led the way in the design and application of computers to the analysis of seemingly unsolvable problems of cryptology. Now the rest of the world has caught fire with enthusiasm in extending the computer's usefulness. We ought to take advantage of this new impetus to extending human analytic capabilities.

~~(C)~~

MINNIE'S MINI:

FIVE YEARS LATER AND I STILL WANT IT!

Minnie M. Kenny
Chief, P16

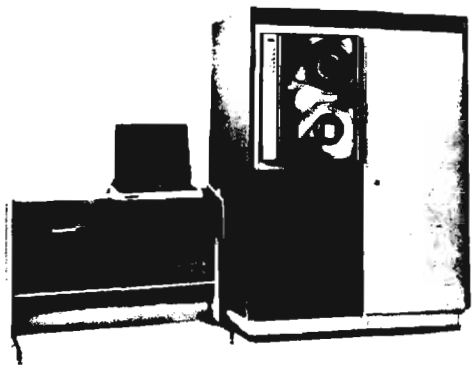
My, my, how the years roll by! In the preceding article, Bill Crowell says that he would like to see personal-sized computers used at NSA. In the December 1973 issue of the B Group publication DRAGON SEEDS, of which she was the founding editor, Minnie M. Kenny said the same thing. That 1973 article is reproduced below, with a brief introductory word by Mrs. Kenny.

Ed.

I definitely agree with Mr. Crowell, as my article in DRAGON SEEDS indicates. Mr. Crowell's article expressed very succintly two points I tried to make to the ALBRECHT Group -- that an analyst must have contact with the materials he is studying and that the personal-sized minicomputers can be used as "powerful new scratch pads" and serve as catalysts for the development of new techniques and applications across the whole vista of cryptologic disciplines. Imagine! Desktop scopes with programmable keyboards and split-screen and scrolling capabilities! They're the answer to a SIGINT maiden's prayers.

It seems like ages ago when it all began. We were still at FANX and had just experienced the nine hundred and ninety-ninth power outage. No COPE, no RYE, no 6700, no *nothing!!!* To top it all off, it wasn't even raining. Now what kind of Providence was that?

We came up with an idea: why not hang a tape drive on that modified PDP-8 called the COPE terminal, boosting its memory by 4K, and declare our independence from Central Control? No way!! We got bottled up in channels and buried under paperwork.



That's when I began dreaming of desk-top terminals for CA applications. Can't you imagine a user-controlled system of minicomputers, say one master and three slaves with an interchangeable hierarchy (to eliminate service interruption when there's a malfunction), and a terminal on each analyst's desk? Why, you'd hardly need cross-section paper and pencils!

One day I stumbled across several idle CRTs. I was nosing around down in C at the time. I *had* to have them. Hooked up to one of the general processors, they'd make an adequate substitute for my dream system. I lost out again. I could pirate the terminals but I couldn't "bootleg" the hook-ups.

About this time, R came on the scene touting minicomputers with blisters. They were developing interactive CA applications. And they wooed me with the promise of the realization of my dream. We formed a committee which formed a study group which formed into teams which inspected CA processes in B. The results were published in a huge compendium called the ALBRECHT Study, but. . . *I still want a mini!*

~~(C)~~

NSA-crostic No. 15

By A.J.S.

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

DEFINITIONS / *WORDS*

A. Escort — 121 21 43 52 95 107 137 163

B. "---------- of Texas" (2 wds) — 29 37 54 101 130 145 211 22 105 122

C. Loathed — 48 4 33 79 134 152 210 247

D. Born — 60 229

E. Genus of snakes comprising the anaconda — 8 86 123 156 228 57 226 230

F. "If I hadda knowed that you'da wanted to of went, I'da seed that ----------" (cited in H. L. Mencken's *The American Language*) (6 wds) — 26 34 72 109 108 186 215 232 67 99 32 179 199 164 243 17 144

G. It sometimes takes people a long time to learn that there's no such thing as --------- (2 wds) — 2 155 182 218 225 19 87 173 200

H. Ballet by Word L (2 wds) — 13 42 204 220 234 28 88 142 169 175 227 250 71 151 24 126 190

I. Bury — 1 47 214 241 23

J. "Alice's ----------" — 7 53 168 202 172 106 70 77 162 233

K. American revolutionary figure (1741-1801) (2 wds) — 171 6 16 56 82 103 127 138 161 207 221 248 44 61

L. American composer (1900-) (2 wds) — 39 64 149 150 176 242 35 85 132 80 183 102

M. Lizard-like animal, found in water or damp places — 10 97 139 209

N. Capital of one of the Soviet republics — 174 30 104 153 246 65 114 147

O. Beloved — 213 3 50 93 135 195 148 117 244 25

P. Civil War general; commanded Confederate left in Battle of Gettysburg — 110 5 125 45 191

Q. Decrease — 236 98 237 31 219 178 11

R. Clumsy — 224 185 113 217 239

S. Type of roof — 141 12 59 75 129 116

T. Get the better of — 158 90 181 206 140 170

U. Extend — 249 160 81 166 194

V. In children's games, the player whom the other players oppose — 188 20

W. The Indian who brought the first electric power line to his tribe's communal outhouse was the first person ever to wire ---------- (5 wds) — 18 49 69 91 133 157 9 112 136 187 192 223 235 245 14 46 124 196 63 167

X. Ballet set to music by Chopin (2 wds)

Y. G. K. ---------- (1874-1936)

Z. Excel

Z_1. Great quantity

Z_2. "Creme de ------"

Z_3. Interrogatory interjection

Z_4. "Blue ---"

Z_5. Teased good-naturedly

55 84 180 212 203 197 216 143 15 222 128 51

111 68 205 27 94 231 159 115 120 40

66 131 92 41 58 208 36 198

189 100 74 83

38 193 73 89 165 146

154 240

119 76 238

78 96 184 62 118 201 177

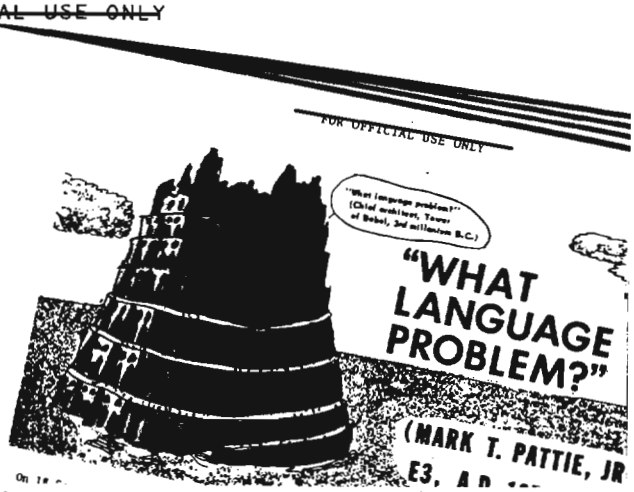
1 I	2 G		3 O	4 C		5 P	6 K	7 J	8 E		9 W	10 M	11 Q		12 S									
13 H	14 W	15 X	16 K	17 F		18 W	19 G	20 V	21 A	22 B	23 I	24 H	25 O	26 F										
27 Y	28 H	29 B	30 N	31 Q	32 F		33 C	34 F		35 L	36 Z	37 B		38 Z_2	39 L									
40 Y		41 Z	42 H	43 A	44 K	45 P		46 W	47 I	48 C		49 W	50 O		51 X									
52 A	53 J	54 B	55 X	56 K	57 E	58 Z		59 S	60 D	61 K		62 Z_5	63 W		64 L									
65 N	66 Z	67 F	68 Y	69 W	70 J		71 H	72 F	73 Z_2	74 Z_1	75 S	76 Z_4	77 J	78 Z_5	79 c									
	80 L	81 U	82 K		83 Z_1	84 X		85 L	86 E	87 G	88 H	89 Z_2	90 T	91 W	92 Z									
93 O	94 Y	95 A		96 Z_5	97 M		98 Q	99 F	100 Z_1	101 B	102 L		103 K	104 N	105 B									
106 J	107 A		108 F		109 F	110 P	111 Y	112 W	113 R	114 N		115 Y	116 S	117 O	118 Z_5									
	119 Z_4	120 Y		121 A	122 B	123 E	124 W	125 P	126 H	127 K	128 X		129 S	130 B	131 Z									
132 L	133 W		134 C	135 O	136 W	137 A	138 K		139 M	140 T	141 S	142 H		143 X	144 F									
145 B	146 Z_2	147 N	148 O	149 L		150 L	151 H		152 C	153 N	154 Z_3	155 G	156 E	157 W	158 T									
159 Y	160 U		161 K	162 J	163 A		164 F	165 Z_2	166 U	167 W		168 J	169 H	170 T										
171 K	172 J	173 G	174 N		175 H	176 L	177 Z_5		178 Q	179 F	180 X	181 T	182 G	183 L										
184 Z_5	185 R		186 F	187 W	188 V	189 Z_1		190 H	191 P	192 W	193 Z_2		194 U	195 O	196 W									
197 X	198 Z		199 F	200 G	201 Z_5		202 J	203 X	204 H	205 Y	206 T	207 K	208 Z	209 M	210 C									
211 B	212 X		213 O	214 I	215 F	216 X	217 R	218 G	219 Q		220 H	221 K	222 X		223 W									
224 R	225 G	226 E	227 H	228 E	229 D		230 E	231 Y	232 F	233 J	234 H	235 W	236 Q		237 Q									
238 Z_4		239 R	240 Z_3	241 I		242 L	243 F	244 O	245 W	246 N	247 C	248 K	249 U	250 H										

A.J.S.

(Solution next month)

AS I WAS SAYING TWO YEARS AGO...

Mark T. Pattie, Jr.



Never underestimate the power of the press, even if it only has a negative effect. In the May 1976 issue of CRYPTOLOG I had an article on the "language problem" within NSA and, if I had known then what I know now, I would not have submitted it, for matters have now gone from bad to worse.

In the article I suggested that the language problem might well be solved if Agency powers-that-be would see fit to reward good linguists with tangible items like promotions. Evidently the article struck a nerve, for disparity between linguist promotions and those for others, such as electronic engineers, has increased.

But what about the latest solution to the "language problem" -- hiring high school graduates to be trained as linguists? It will be quite some time before the results of this move can be evaluated, so I am in no position to state positively that it will not work. Still, I find it difficult to be optimistic, for I have been around long enough to remember the similar experiment with high school students back in the 1960s. Surely M3 has figures showing how many were trained and what became of them. If memory serves me right, there were few who completed the program and I have no way of knowing how many, if any, are still with the Agency and in language work.

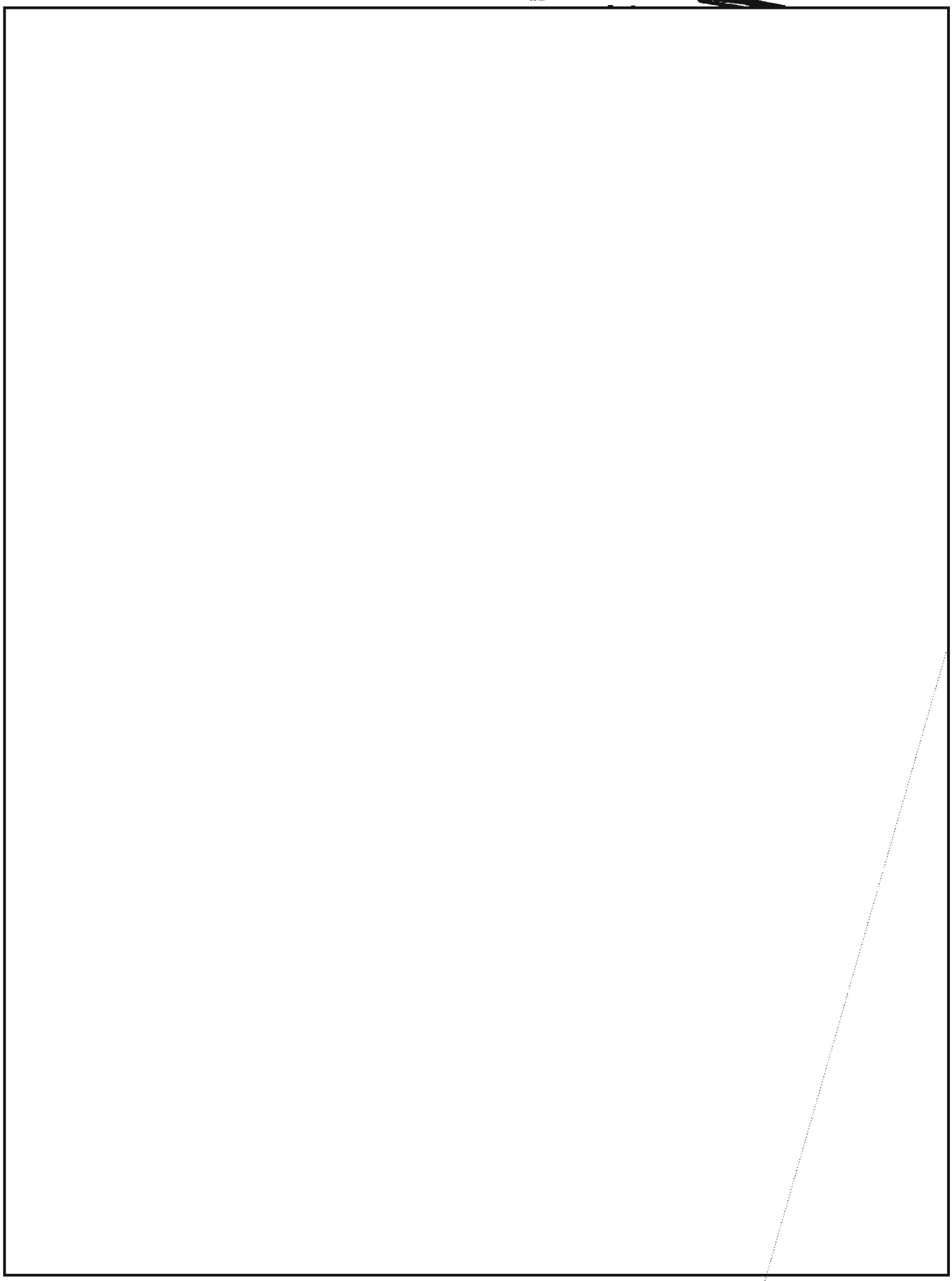
Still, let us assume that the exercise will be completely successful. Then, why don't we hire high school graduates to be trained as engineers or mathematicians? After all, if it would work for one skill, it ought to work for all. Somehow I doubt that those who hire mathematicians and engineers would allow that to happen.

So, how did it happen for linguists? I can only suspect that what I said in the earlier article continues to hold. Those who make decisions about linguistic capability are not linguists and they remain convinced that it takes little to become one. I would think that the fiasco of President Carter's interpreter in Poland might disabuse them of that notion.

P.L. 86-36

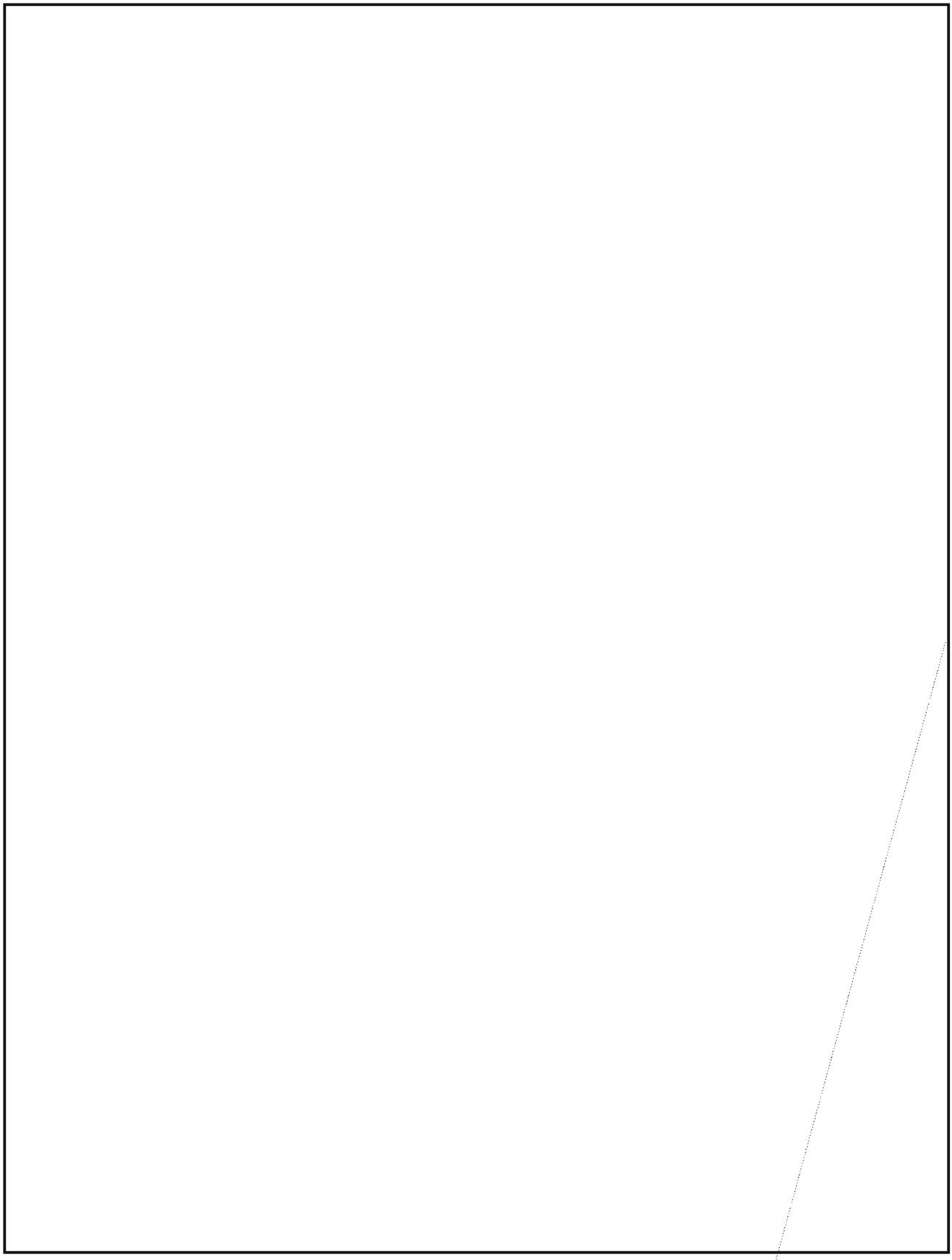
There is an old cliche, "You get what you pay for." For years those who make decisions about hiring for the Agency have managed to use that cliche as a lever to have engineers and scientific personnel hired at higher grades or at higher levels within grades. Now, to use another cliche, "The rich will get richer and the poor will get poorer." Linguists will enter at the lowest possible grades and will be competing with those who are being hired many grades above them, with little -- actually, no -- hope of ever catching up. This will be a self-perpetuating situation, for the time will come when only engineers and scientists will have high enough grades to be considered for appointment to senior management positions and they will continue to make the decisions affecting linguists.

If I sound bitter, it is only because I am. Our product, so dependent upon the efforts of linguists, is bound to suffer as senior linguists leave, and I do not see anything but a downhill trend in the years ahead if the present policies remain unchanged. You *do* get what you pay for!



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

~~SECRET SPOKE~~



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

CELTIC LANGUAGES TODAY

(A LOOK AT WELSH AND GAELIC)

Llanfairpwllgwyngyllgogerychwyrndrobwll-llantysiliogogogoch. It is undoubtedly the longest place name in the world, and it hangs over the train station of this village in Anglesey, North Wales, only a few miles distant from the village of Llanfairfechan, where I stayed in the summer of 1977. The name means "St. Mary's Church, in a hollow of white hazel, close to a rapid whirlpool and St. Tysilio's Church, and near a red cave." (It is usually mercifully abbreviated to Llanfair P. G.)

I had come to Wales to learn more about the Welsh language and to collect materials in that language. Later I would go north to Scotland and try to do the same with Gaelic. The events that led to this pilgrimage, and what I discovered there, are the topic of this article.

Before discussing the difficulties that a student of Welsh encounters (using words of more manageable length than the one above), I would like to say a few words about Celtic in general.

We have witnessed a revival of interest in Celtic (pronounced "*K*el-tick," not "*S*el-tick" -- there is no *c* pronounced as *s* in any Celtic language) studies in recent years. As I looked for the reasons behind this upsurge in interest, I came up with several possible ones:

- the *Roots* search, not limited to blacks, but involving people of all ethnic groups;
- increased publicity. In May 1977 *National Geographic* published a beautifully illustrated article on the Celts by Merle Severy, including a map of Celtic Europe. The map shows that there were Celtic settlements as remote as present-day Turkey, where the Galatians lived. (St. Paul wrote an epistle to the Galatians and it eventually became part of the New Testament.)

  There is also a greater awareness of Celtic language (and mythology) because of the tremendous success of J. R. R. Tolkien's books. *The Hobbitt*, *The Lord of the Rings*, and, more recently, *The Silmarillion* draw upon the wellspring of Icelandic and Celtic lore. Tolkien liked Welsh better than any other language, and used it as a basis for many of the words in his artificial languages. As people became aware of his sources, their own interests in these subjects were stimulated.
- Another reason for the revival of interest is that the field has not been overworked. There is still plenty to do. In my own field of Hebrew -- especially in the area of the Bible -- scholars have gone over the same ground many times with a fine-toothed comb. But with Celtic the situation is just the opposite. Dr. Robert Meyer of Catholic University, in Washington, once said that every time he "puts down his spade," as it were, he comes up with something new.
- Last but not least, one may mention the conflict in Northern Ireland, which has called attention to all things Irish.

My own interest in Celtic languages can be traced at least in part to a chance remark made by Agency linguist John Murphy. He pointed out that in many ways Irish resembles Hebrew and the other Semitic languages in its structure. Some scholars had actually gone so far as to suggest

Based on a talk given in September 1977 to SIGTRAN (the Crypto-Linguistics Association's Special Interest Group on Translation).

that the insular Celtic languages had been influenced by some Afro-Asiatic substratum. John Murphy referred to such features as a "construct state" and conjugated prepositions. Later on, when I took Dr. Meyer's course in Old Irish, I was able to spot more similarities, in addition to the ones John Murphy had mentioned. Here are some examples, taken from the "Scela Mucce Meic Datho" (The Story of Mac Datho's Pig):

Construct State

Old Irish: *"Ailbe ainm in chon."* "Ailbe was the name of the dog," lit. "Ailbe name the dog," exactly parallel to "Ailbe shem ha-kelev" if we were to translate it into Hebrew.

Verb-Subject-Object Word Order

Old Irish: *"Imdīched in cú Laigniu huili."* "The dog defended all Leinster," lit. "Defended the dog Leinster all-of-it." In classical Hebrew one would say, "Vayagen ha-kelev ʿal Leinster kullah," preserving the same word order. Such an order is unusual in a European language.

Conjugated Prepositions

The Old Irish word for "with" is *la*. Conjugated with pronominal suffixes, this becomes *lem, lat, leiss*, etc. In Hebrew and Arabic, most prepositions can likewise be conjugated.

Anticipatory construction for genitive

This feature is shared by both Old Irish and Aramaic. (Late Hebrew has it as a result of Aramaic influence.) Old Irish: *"Ba lán Hériu dia airdircus in chon."* "Ireland was full of the fame of the dog," lit. "Was full Ireland of-his fame of the dog." Cf. Modern Hebrew: "Kalbō šel ha-ʾīš," lit. "his-dog of the man," = "the dog of the man," "the man's dog."

Yet, from a lexical standpoint, the theory that insular Celtic had some kind of Semitic influence -- say, from the Phoenicians -- finds no support. Aside from a few chance resemblances, there is no trace of it. One thinks readily of the Arabic loan-words in Spanish, Turkish, or Persian; the Spanish words in Basque; or the enormous influence exerted on English by Norse (from which even our third person *th-* pronouns were borrowed). The fact that nothing like this can be seen in Celtic makes its connection with Hebrew very doubtful.

I should now like to give an overview of the Celtic languages, both living and extinct, before concentrating on Welsh and Gaelic to "take their pulse," as it were, to determine where they are healthy and where not, and what is being done to keep them alive.

The Celtic languages can be divided into two groups: insular and continental (see Fig. 1). The continental Celtic languages were once very widespread over the European continent, but little is known about them. Caesar wrote about the Gauls, and there are some Gaulic inscriptions, but little else remains.

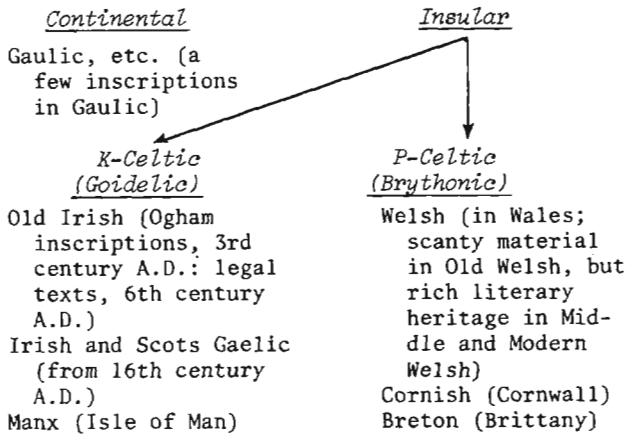


Fig. 1

The insular branch is divided into K-Celtic (Q-Celtic) and P-Celtic because of a split that occurred from the Indo-European consonant **kw-*. In Irish the labialization was lost, so that only the *k* sound remained; cf. the Irish word for "head," *ceann*, as in the name Kennedy, which literally means "ugly head." In Welsh, on the other hand, the word for "head" is *pen* as in "penguin," which literally means "white head."

Both Manx and Cornish are extinct. The last Cornish speaker is reported to have been a fisherwoman named Dolly Pantreath of Mousehole (pronounced *mōōsə'l*), who died in 1789. Another researcher, however, has claimed that its last speakers were Cornish miners who took part in the California gold rush of 1849.

As for Manx, there were still four persons alive in 1954 who spoke that language, and they were very elderly at the time, so we may safely assume that Manx too is by now a dead language.

Turning to Gaelic, we find a living language, but you may have to go out of your way to hear it spoken.

In Edinburgh I attended a Gaelic church service on a Sunday afternoon at the Highland Tolbooth St. John's Church. The people were most friendly; they bade me "a hundred thousand welcomes," or *"Ceud mile failte,"* as they say in Gaelic, and I made the acquaintance of a kilted gentleman and his wife who put me in touch with the right organizations and publishing houses, so that I could acquire more Gaelic materials. The chap had even studied a bit of Hebrew, as it turned out, so we found that we had some other common ground and hit it off very nicely right from the start.

At his recommendation I visited the School of Scottish Studies at the University of Edinburgh. School was out for the summer and they were operating on a skeleton crew, but the visit turned out to be worthwhile nonetheless. I learned that they had recorded thousands of

hours of Gaelic speech on tape and that they publish an attractive bilingual magazine, *Tocher* (Dowry). It appears 3 times a year and costs only 40 p an issue. Here you can find stories, songs, and traditions from the school's archives.

There is also a publishing house called *"Gairm"* (Word) which prints books and manuals in and about Gaelic (see bibliography).

A complete Gaelic course is available on tape from National Extension College in Cambridge, England, for about $50.00, and a number of other tuitional aids are available on both disks and cassettes (see bibliography).

But to hear Gaelic spoken freely and naturally, one must go to the islands, to a place such as Harris on the Isle of Lewis, so far north that it never gets dark in the summertime, and where people are not subjected to as much English influence. Even television has not made great inroads among the people as yet, for the reception is poor in this region. A great deal of linguistic and sociological research is being conducted on these people. For example, a book was published in 1977 by Kenneth MacKinnon, *Language, Education and Social Processes in a Gaelic Community*. If you are interested in such minute details as the percentage of male Gaelic speakers using the formal second-person pronoun *sibh* to their wives (p. 19) or a poll that asks of the Harris community, "Do girls tend to keep their Gaelic in use better than boys?" (p. 163), then this is the place to turn to.

But in many ways Gaelic is losing ground. Gaelic broadcasting, already infrequent, has recently been cut back even more by the BBC, causing an uproar among Gaelic supporters. An appeal was made to the BBC and a final decision is pending.

Welsh

When we turn our attention to Welsh, the picture has a rosier, healthier look about it. Here we are dealing with a much larger number of speakers -- perhaps around 2 million -- and their firm resolve to keep the language going. Welsh is also easier than Gaelic in that it is more "phonetic" (it is pronounced just about as it is written, while Gaelic is like English in that its spelling includes silent letters, etc.). Radio and TV programs abound; I was able to tape a number of broadcasts during my stay in Wales.

But there is a difficulty in learning Welsh: the initial mutations. Most languages with which we are familiar introduce changes at the *end* of the word (the declensions and conjugations of Latin or Russian, for example). Now imagine a language in which the word changes at the *beginning*. How would you ever find it in the dictionary? You couldn't, of course, unless you knew something about the grammar! There is an excellent example of this in the name of the village where I stayed -- Llanfairfechan. Now, Llanfairfechan means literally "Little Church of St. Mary's." *Llan* is "church" or "parish," a feminine noun. *Fair* is really *Mair* (Mary), but after *llan* the *m* changes to *f*. And the word *fechan* can be found in the dictionary only under its masculine form *bychan*, "small." This is known as the *soft mutation*.

Besides the soft mutation there is a *nasal mutation* involving six consonants:

	Labials	*Dentals*	*Velars*
Voiced	b → m	d → n	g → ng
Unvoiced	p → mh	t → nh	c → ngh

This generally happens after the words *fy* ("my") and *yn* ("in"). Thus, *pen*, "head," but *fy mhen*, "my head."

Finally, there is a *spirant mutation* affecting the consonants *c*, *p*, and *t*. This occurs after the word for "her," *ei*, e. g. *ei phen* = "her head." (To use an English example, "peasant" would become "her pheasant"!)

But aside from this difficulty there is really no problem. The English loan words abound, and the imprint of English is profound in other respects as well; once, in a child's story, I came across the words *Oedd Pwll mewn picil*, "Pwyll was in a pickle," describing one of the characters (Pwyll, hero of the First Branch of the Mabinogion) who had gotten himself into some difficulty. This is hardly the sort of thing that one would expect to find in the original Mabinogion, or in any other writing true to the Welsh spirit!

There are also several Welsh newspapers (such as *Y Herald Cymraeg*), indicating that here again the situation is healthier than for Gaelic, which only has an occasional page or column in an English-language newspaper published in the Hebrides.

It is also easier to find Welsh books. There is, for example, a set of Welsh comic books, designed to teach the language and make it seem like fun; and, though some of the humor is ribald and one senses that beer-drinking must be an important part of the culture, the comic books are nonetheless an effective medium for the acquisition of the colloquial language. There are also graded readers to help one along after he has mastered the rudiments of the language (see bibliography). I was even able to pick up attractive children's books such as *Alice in Wonderland* and *Snow White and the Seven Dwarfs*. The story of Snow White with its Disneyesque illustrations takes place between the Welsh village of Llanfair y Lli and Llanfair y Llwyn. It was also possible to pick up an excellent Welsh dictionary at a very reasonable price, in contrast to the Gaelic one which cost £8 and which I therefore decided to postpone buying.

As one travels the motorways, one sees Welsh signs everywhere. In the June 25, 1977

issue of *The Economist* in an article entitled "How Bilingual Was My Valley," we are told that the government is spending £10 million to cover Wales with bilingual signs. The article goes on to say:

> "The Welsh Language Society's long efforts at direct action -- raids on television transmitters, bonfires of English-language documents and sit-ins -- have resulted in the Welsh population receiving dual-language versions of all kinds of official forms, from driver's licenses to telephone bills, with even the *p* for pence translated into *c* for *ceiniogau*."

So it appears that an all-out effort is being made for Welsh. In contrast to a tiny corner devoted to Gaelic books at a Scottish book seller's, one finds entire shops in Wales that specialize in Welsh books. In one such shop in Caernarvon the owner, Mr. Eric Jones, told me that after all the tourists go home at the end of August, one hardly hears a word of English spoken in the town until they return in April.

Here, then, is a field that has much to offer the language student. Whether one delves into the medieval or modern phase of Celtic, there is a wealth of interesting literature. It is a field that is not overcrowded and in which much basic work remains to be done. But when one looks at those universities in the United States that offer Celtic languages, one finds that there are only two American universities that have Celtic departments: Harvard University and Catholic University (Dr. Robert T. Meyer, of Catholic, is the only Professor Emeritus of Celtic languages in the country). Elsewhere, Celtic languages are offered within the departments of English or Modern Languages, as is the case at the University of Texas, for example.

Catholic University has an outstanding Celtic collection, having absorbed the libraries of Professor Joseph Dunn and Major William B. S. Smith. These include a complete set of the *Revue celtique* and the rare *Annales de Bretagne*. But the department has remained small due to the shortage of money (they have a $50,000 endowment fund, the annual interest from which comes to only $3000 or so.) People are attracted to the course for a variety of reasons -- some are medievalists or majors in English or linguistics. A small number are actually majoring in Celtic. And then there are people like myself -- people already established in some field who, through a series of circumstances, have caught the Celtic fever and enjoy the subject as a pleasant and rewarding pastime.

Readers who would like to receive a copy of the bibliography prepared by [redacted] *can get one by writing to: CRYPTOLOG, P1, or by calling the editor on 5236s.* (U)

Letter to the Editor

To the Editor, CRYPTOLOG:

I am sure there are many opinions on the questions posed by [redacted] in his article "What Ever Happened to COPES?" (CRYPTOLOG, January 1978). Perhaps the questions that should be answered is: What has COPES done for *us*? Have we increased our understanding of the target? Has output level been maintained with less collection resources? Is collection management easier? I believe the middle managers (some of whom must have been workers in early days of COPES) would have "taken hold of COPES and made it their own" if it had demonstrated its utility.

P.L. 86-36

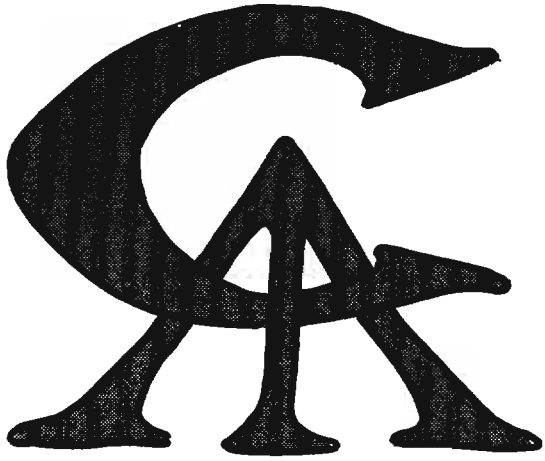
EO 1.4.(c)
P.L. 86-36

[redacted]

Eugene A. Gilbertson,
[redacted] ~~(C - CCO)~~

P.L. 86-36

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



News of the Communications Analysis Association

By [redacted] P14

P.L. 86-36

How do you like our new logo? As mentioned in last month's News of the CAA, the winning entry was sent in by [redacted] We had hoped to have a professionally drawn version of it for this month's issue, but we were late in asking Graphics to do it for us. In the meantime, to appease your curiosity, here it is, in a version based on the winner's original sketch. In case you don't know why you like it so much, Hugh explains that "The design is the basic monogram based on Classic Roman Capitals, arranged to give an impression of breadth and upward motion."

(U)

Monthly Meetings

The CAA is on the move again, in all its breadth and upward motion! Our board meets once a month, usually around the end of the month, but the exact time and room change from one month to another. But the meetings are open to all, members or others. If you want to come try and look us over before deciding whether to associate with the likes of us, please do so. We won't even swear you to secrecy about all the wild things that go on at the meetings. If you're afraid to come alone, bring a friend. Where and when? To tell you the truth, as I write this (in April) I don't really know. But as you *read* this (in June), you can find out. Just check with your nearest CAA member, or with any of the CAA Board members listed below. Or, if you're already a member, watch for the notices arriving in your in-basket.

(U)

[redacted]

~~(SC)~~

CAA Program Committee

Our Program Committee, chaired by [redacted] has been busy, too. The committee includes:

[redacted] 5617s
8379s
3505s
4226s

In addition to the monthly meetings of the Board, bimonthly meetings of the Special Interest Group on Cryptologic History, and operational briefs, the Program Committee has lined up the following speakers:

28 June [redacted]

(?September?)

Any ideas for other presentations or other speakers? Let the committee know.

(U)

Meet the CAA Secretary!

[redacted] more generally known as Betty, P.L. 86-36 is currently Secretary of the CAA. She came to an early predecessor of NSA as a French linguist but was shunted to cryptanalysis, where she has dwelt happily ever since. Her assignments have covered problems that are now handled in A, B, and G; she has held technical management positions at section, branch, division, and office staff levels; and she now heads the Cryptanalysis Division in the National Cryptologic School. She is a member of the Crypto-Linguistics Association and of the CAA Special Interest Group on Cryptologic History. She is also an EEO Counselor, President of the Patuxent Business and Professional Women's Club and editor of its Newsletter; the former editor of the WIN (Women in NSA) *Newsletter;* former Cryptanalysis Editor of CRYPTOLOG, and Rewrite Editor of its predecessor *Dragon Seeds*.

(U)

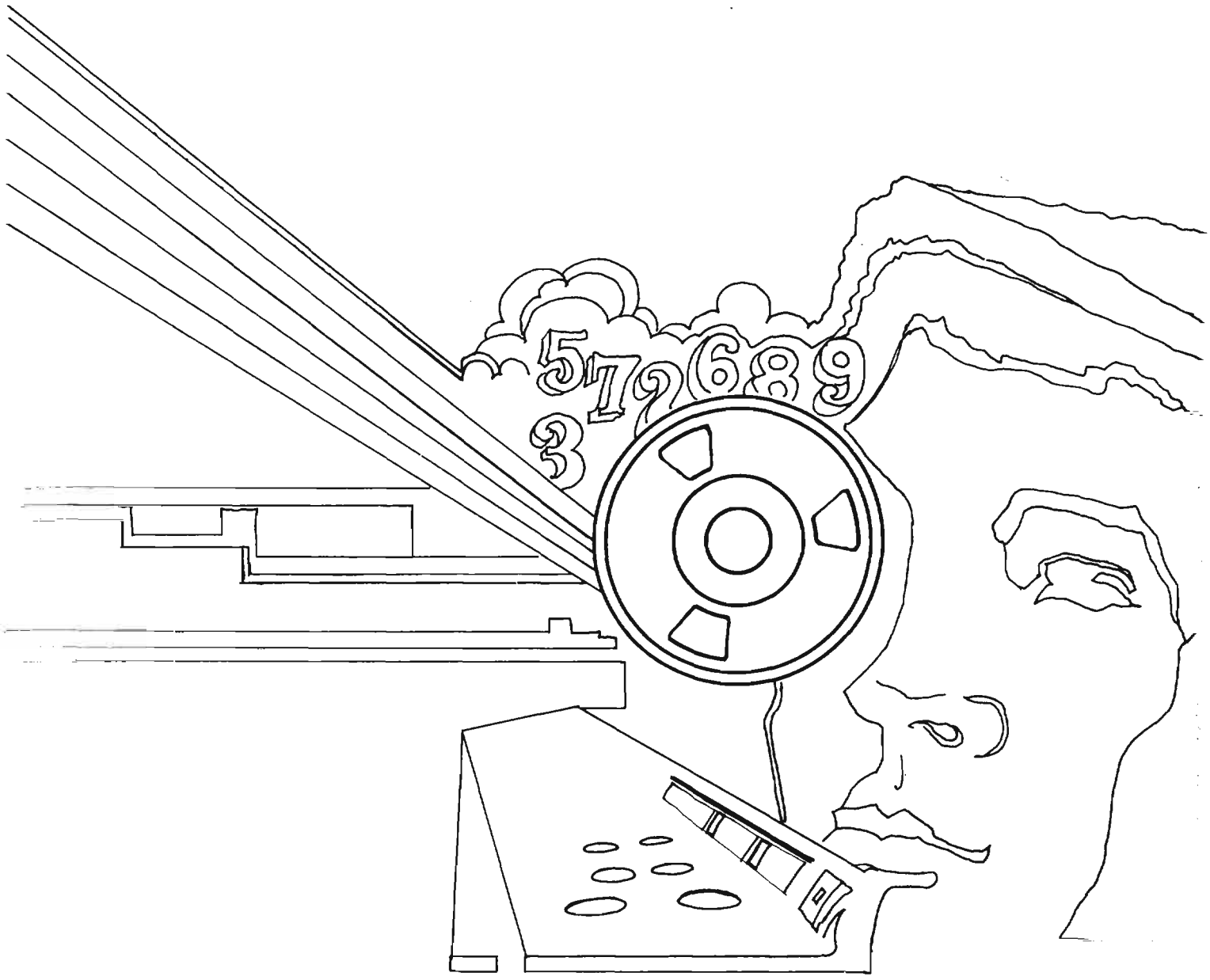
Communications Analysis Association:

President	David Gaddy	3247
President-elect	Frank Porrino	5879
Secretary	[redacted]	8025
Treasurer	Tim Murphy	3791
Board members	[redacted]	4935
		5991
		3573
		3369

P.L. 86-36

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

P.L. 86-36


5 7 9 6 8 9
3