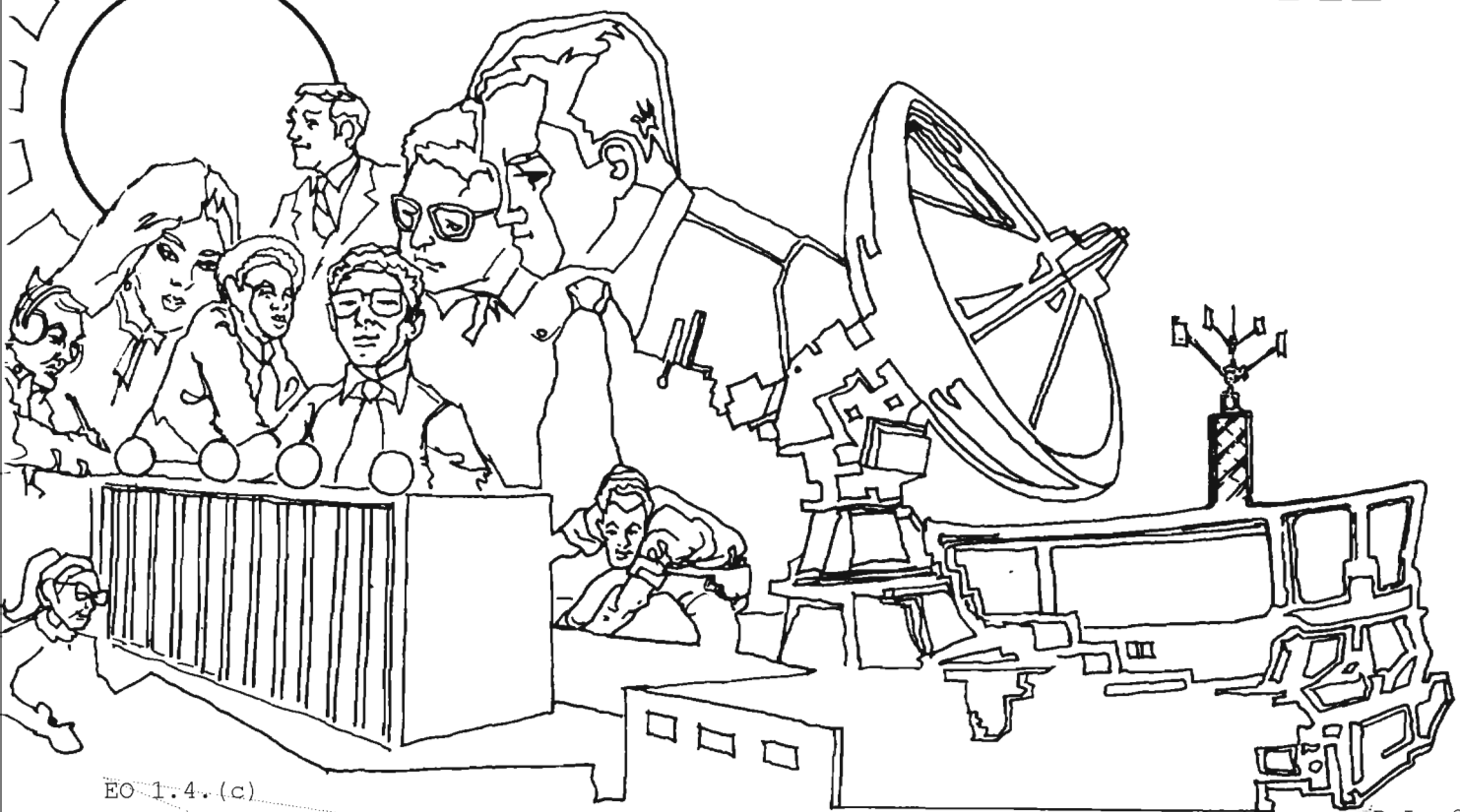


~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

FEBRUARY 1978



EO 1.4.(c)

P.L. 86-36

[REDACTED]	[REDACTED]	1
COLLECTION-SUPPORT T.A. IS NOT FOR EVERYONE	[REDACTED]	7
UNSEEN GO-BETWEEN: CONFERENCE INTERPRETER...	J. Gurin	9
[REDACTED]	[REDACTED]	11
FIRST LADY OF NAVAL CRYPTOLOGY.....	[REDACTED]	14
C.A.A. NEWS.....	[REDACTED]	14
MILITARY CRYPTOLOGIC SUPERVISORS COURSE....	[REDACTED]	15
MORE BEANS.....	Vera Ruth Filby	17
BY-LINES DON'T COST -- THEY PAY!.....	John J. Mollick	19
"NO, WINNIE, YOU'VE GOT IT UPSIDE-DOWN!"....	A.J.S.	20

~~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. 2

FEBRUARY 1978

PUBLISHER

WILLIAM LUTWINIAK

BOARD OF EDITORS

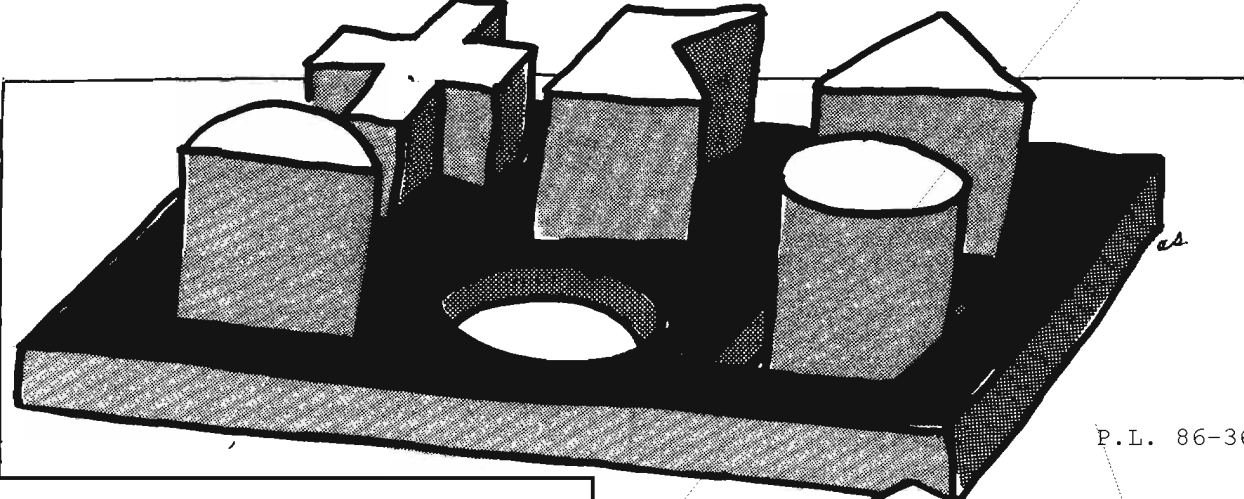
Editor in Chief.....Arthur J. Saleme (5236s)
 Collection..... [redacted] (8955s)
 Cryptanalysis..... [redacted] (4902s)
 Language..... [redacted] (5236s)
 Machine Support..... [redacted] (5303s)
 Mathematics.....Reed Dawson (3957s)
 Special Research.....Vera Filby (7119s)
 Traffic Analysis..... [redacted] (4477s)
 Production Manager.....Harry Goff (4998s)

P.L. 86-36

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

~~TOP SECRET~~

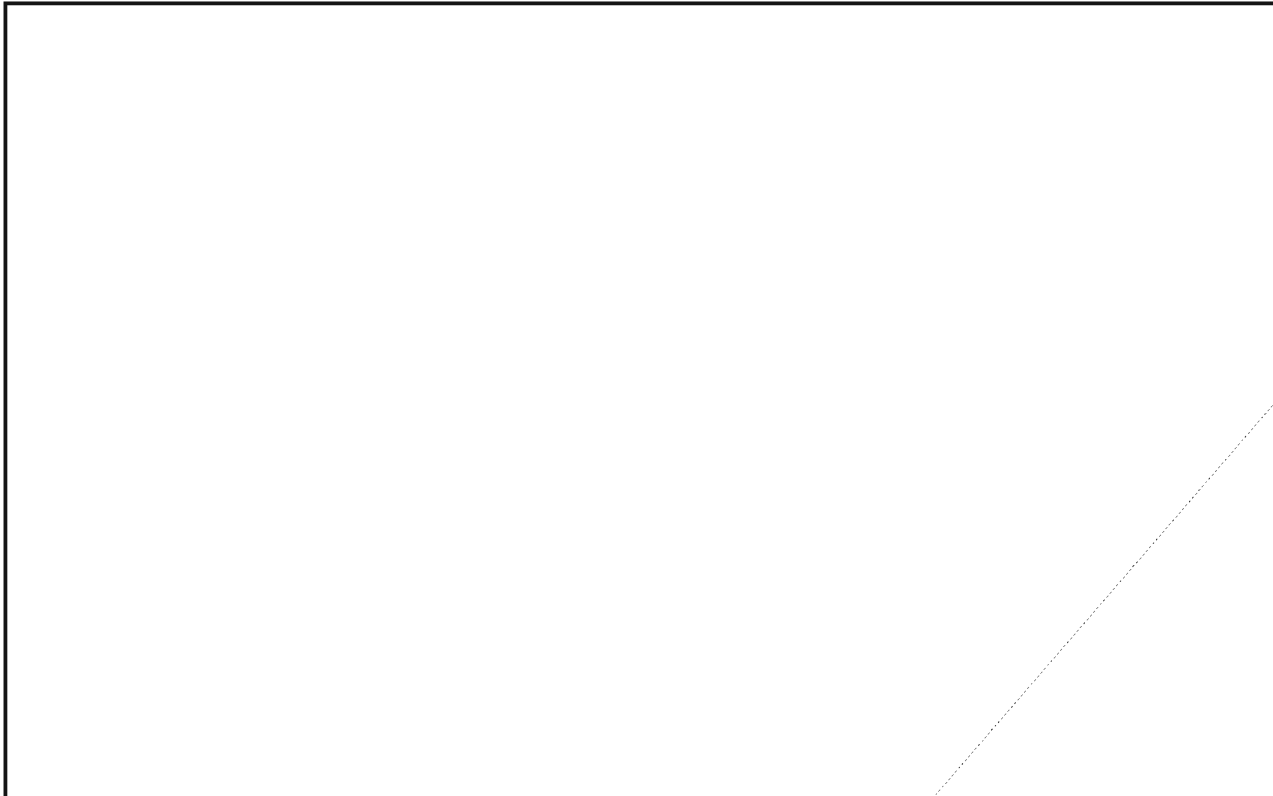
~~TOP SECRET UMBRA~~



P.L. 86-36

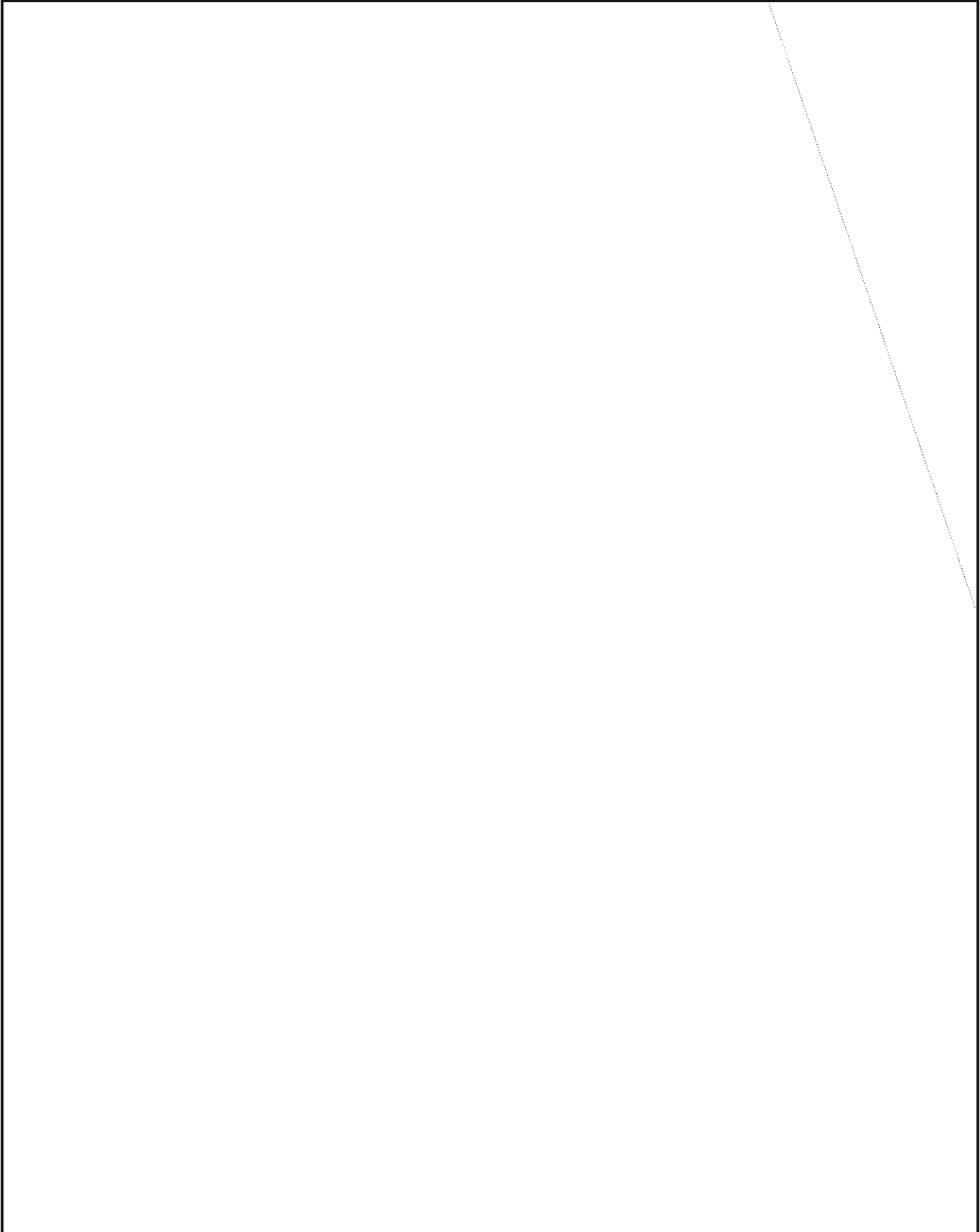


**Square Peg,
Round Hole?**

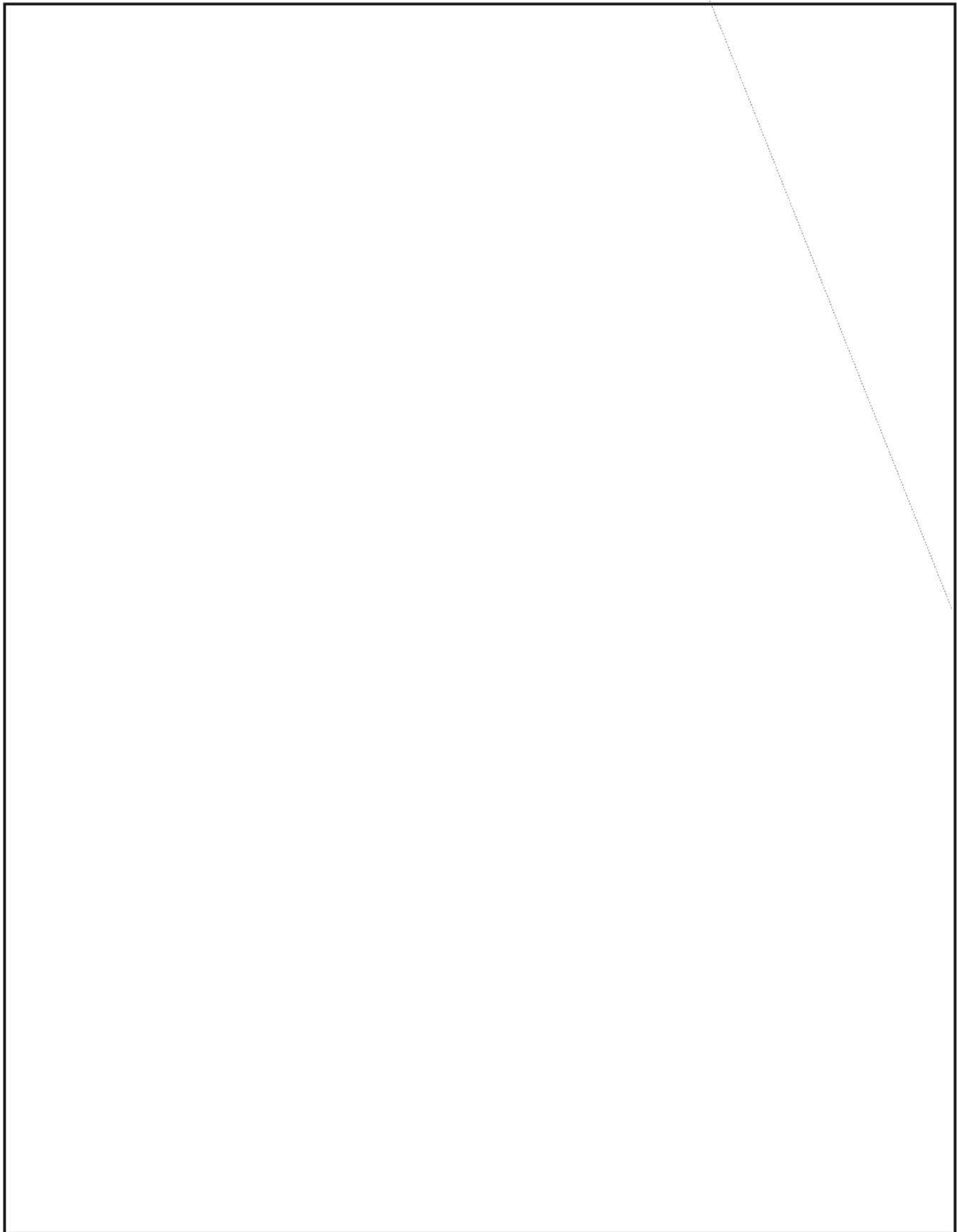


~~TOP SECRET UMBRA~~

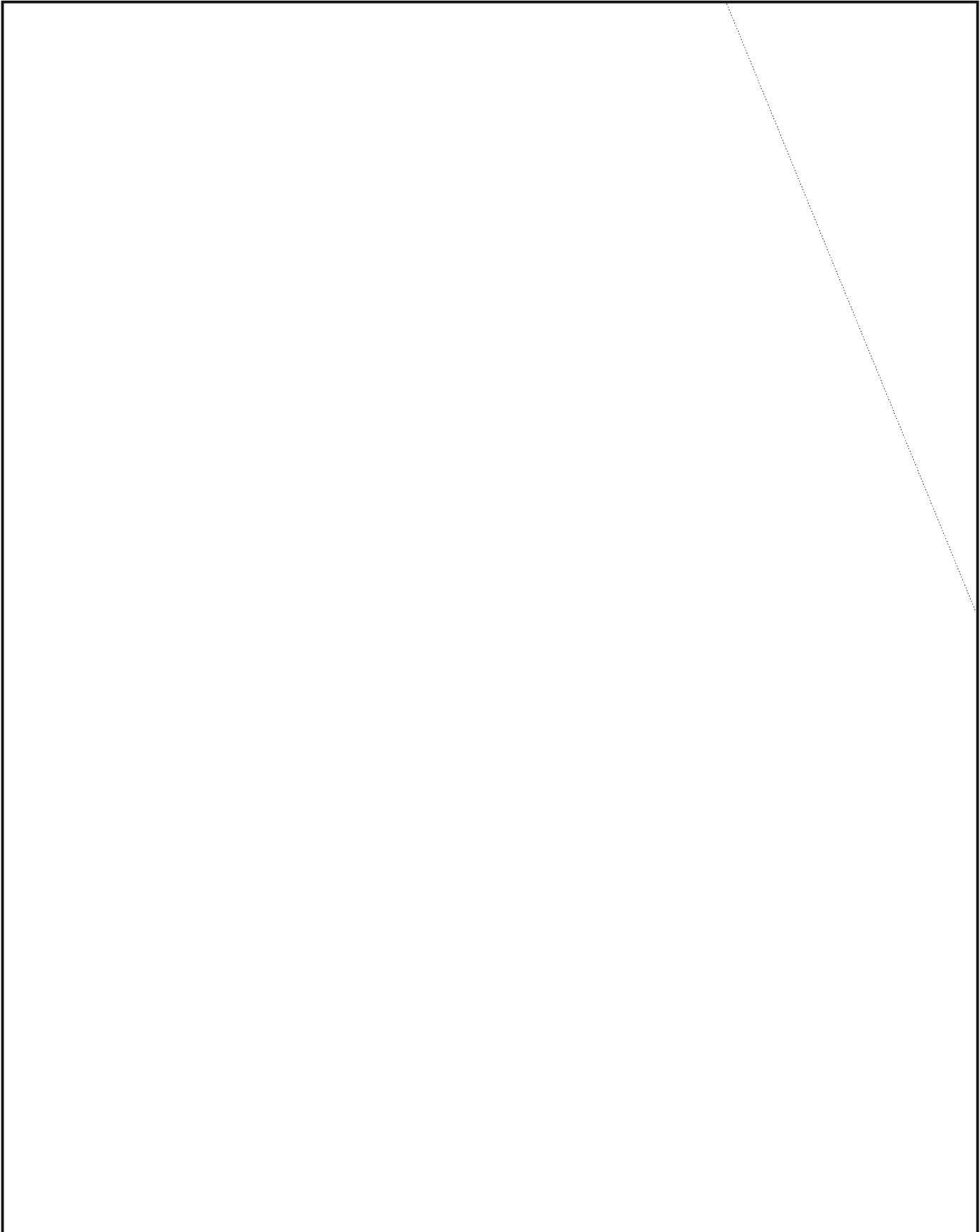
~~TOP SECRET UMBRA~~



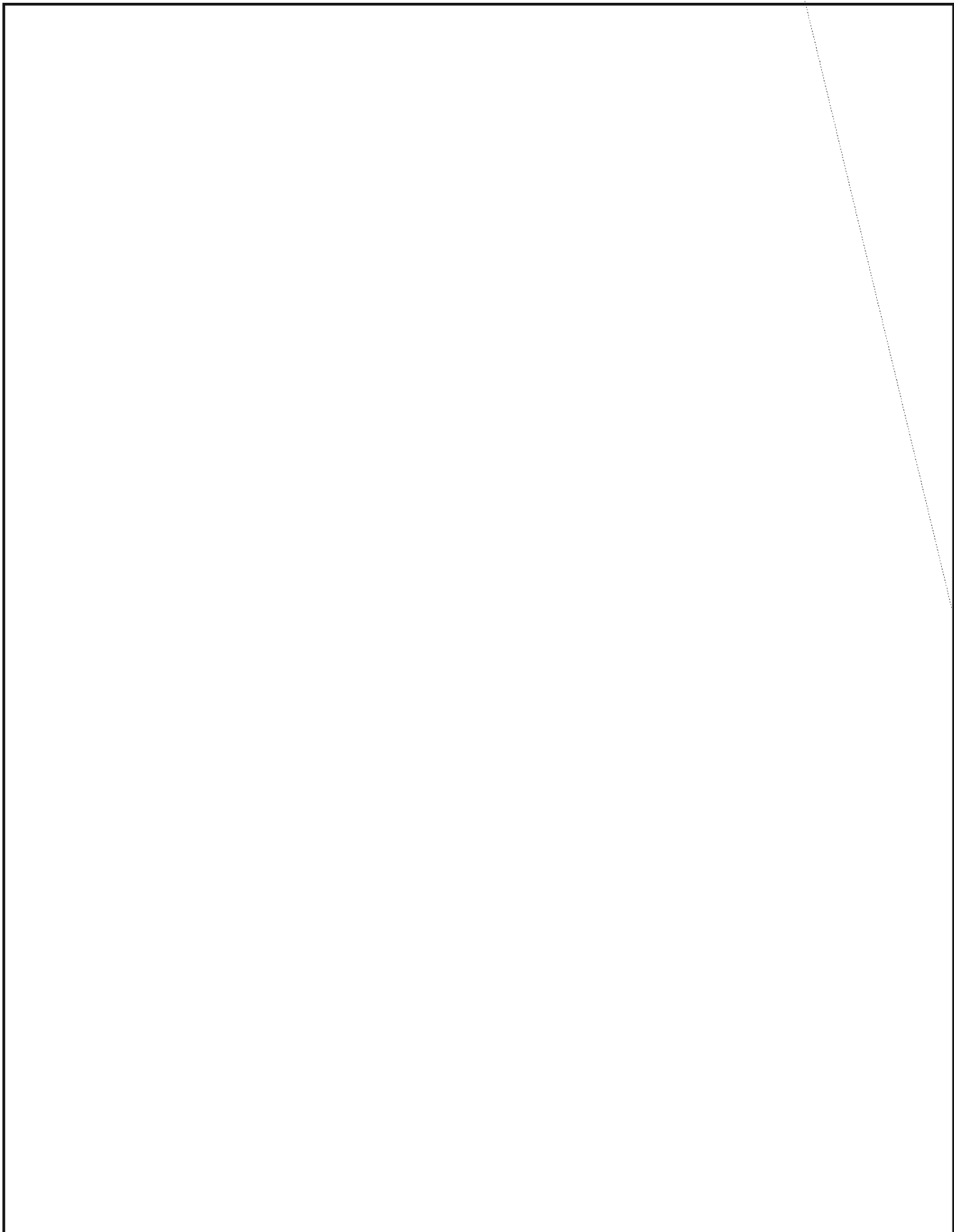
~~TOP SECRET UMBRA~~



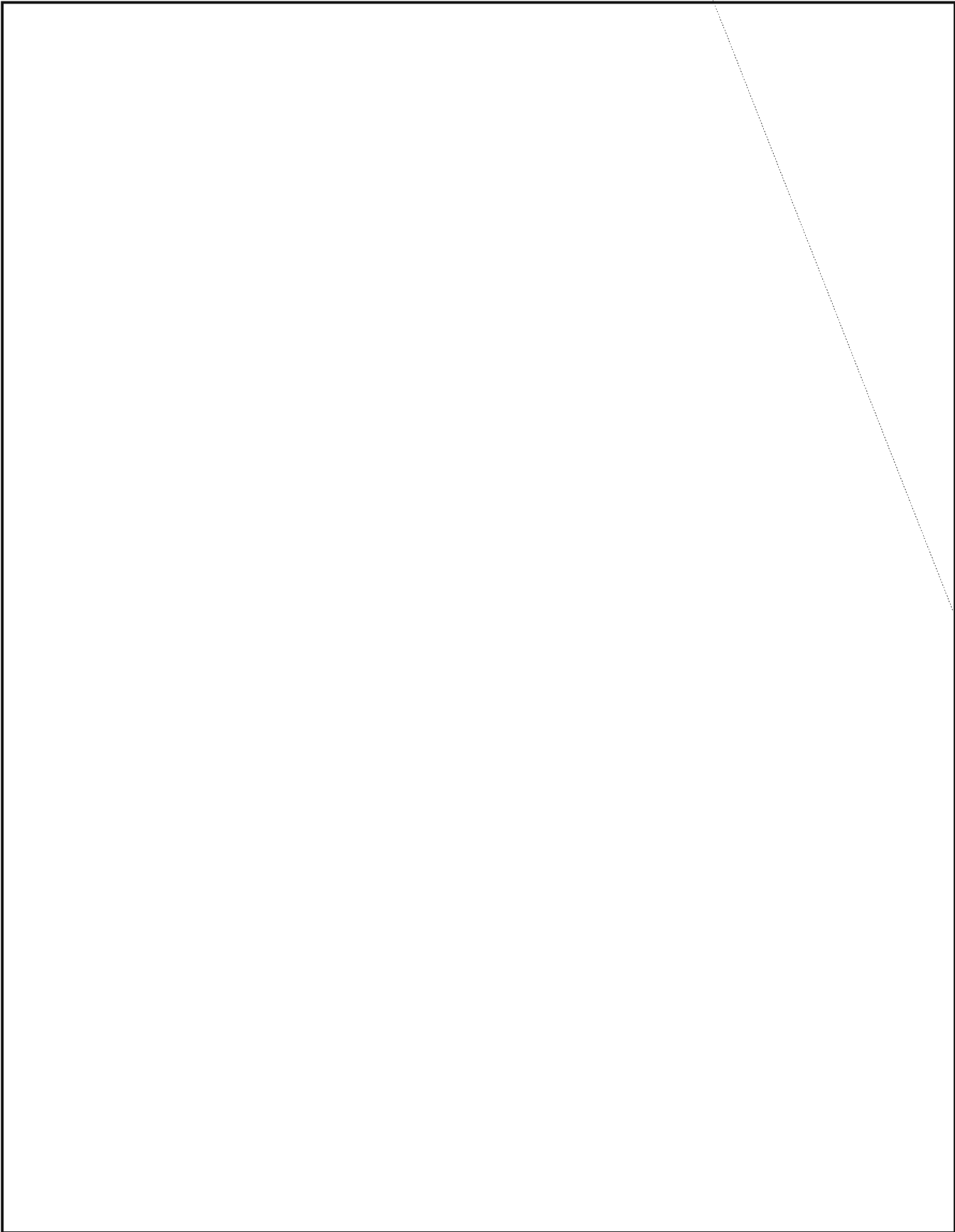
~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~CONFIDENTIAL~~

COLLECTION-SUPPORT TA IS NOT FOR EVERYONE

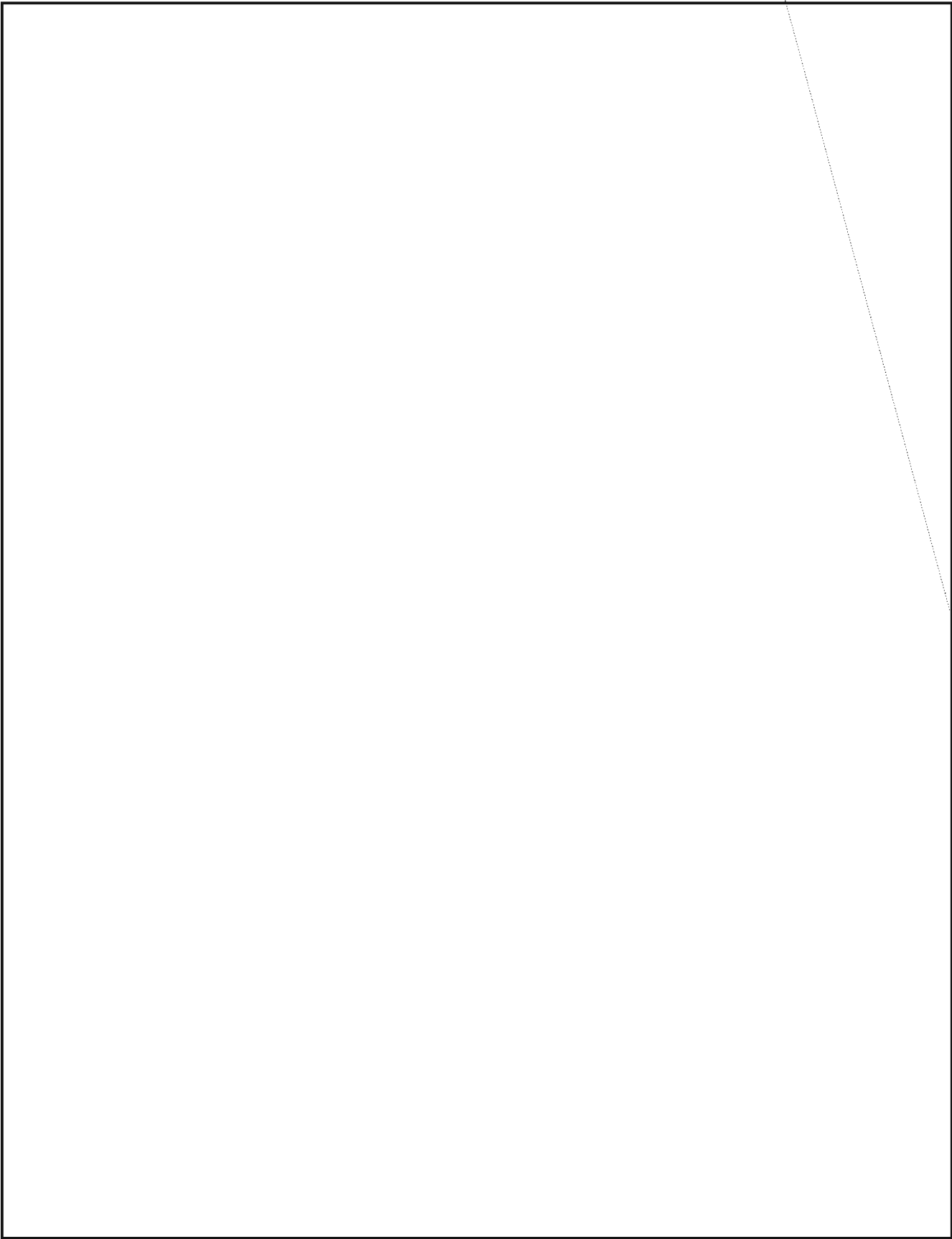
P.L. 86-36



It is often said that the traffic analyst working in a collection-operations area isn't doing traffic analysis. This is because very little in-depth analysis is being performed. Better termed, the work could be called "collection-support analysis." It is a special type of traffic analysis for which not all traffic analysts are well-suited. In fact, it is so different that some might suggest it be considered as a unique career specialty.

Recruitment of individuals with an aptitude for collection-support analysis, in my opinion, should be better defined. Too often, there seems to have been a willingness to accept any traffic analyst willing to work rotating shifts or perhaps willing to take a field-station tour of duty. Unfortunately, the skills needed to be a good traffic analyst do not necessarily transfer into making a good collection-support analyst (CSA). A certain mental persuasion is needed in order to be a competent CSA/TA in a collection-support analysis environment. This person plays a vital role in the collection cycle. He should be the oil and grease in the input, output, and feedback process of the collection cycle. This article will identify the role of the collection-support analyst and attempt to identify what his mental persuasion should be toward his job.

~~CONFIDENTIAL~~~~HANDLE VIA COMINT CHANNELS ONLY~~



UNCLASSIFIED



THE UNSEEN GO-BETWEEN: THE CONFERENCE INTERPRETER

J. Gurin, R5

Conference interpreting, without which there could be little communication among conferees from different countries, speaking different languages, is a young art. Before World War I, it was recognized and accepted that international conferences would be conducted in French, and no diplomat could expect to follow the course of action at such a meeting or be invited to participate actively if he did not possess a respectable command of that language. But during World War I, things changed drastically, and meetings between high-ranking French and British (and, later, American) officers required the services of interpreters.

At a recent NATO symposium on interpreting, it was my good fortune to meet and hear Dr. Jean Herbert, now of Geneva, who is the grand old man of conference interpreting. He has been performing that function for more than 60 years, beginning as a young officer in the French Army who happened to speak fluent English. He told of the Armistice Commissions, at which interpreters did the best they could at consecutive interpretation in French and English around the conference table. By the time of the Peace Conference, held exclusively in French and English, there were about a dozen interpreters who could take down and translate speeches verbatim. Consecutive interpretation was the rule throughout the life of the League of Nations,

and it wasn't until World War II that simultaneous interpretation was introduced. For a long time it was not trusted because the speaker's delegation could not check the translation and because the performance left much to be desired. As a result, consecutive interpretation continued for a number of years in meetings of the United Nations. With the increase in the number of languages used, however, simultaneous interpretation finally won over, and with the availability of competent, professional interpreters, it is now fully accepted.

It is almost inevitable that, in a discussion of highly demanding interpreting tasks, the subject of bilingualism, or the degree of fluency in more than one language, should come up. While they still may argue among themselves about the precise meanings of the term, the professional interpreters rate themselves for their languages as follows: A - mother-tongue proficiency; B - fluent, active proficiency; C - excellent passive knowledge. It seems to be generally accepted that bilingualism means two mother tongues, a rare event even among the interpreters. Dr. Christopher Thiery, who teaches interpreting at the University of Paris, and who demonstrated for us in the course of the conference the skill of a consecutive interpreter of the first rank, maintained that trilingualism, i.e., three mother tongues, was virtually an impossibility. He himself could pass for an Englishman in England and a

UNCLASSIFIED

Frenchman in France and never make a single slip. He admitted that several professional interpreters listed three Level-A languages against their names, but said that, in his opinion, only one might qualify as a true trilingual. This man, a former Spanish aristocrat, had learned his English and French from governesses in his childhood.

In recent years, the role of the conference interpreter, his specific professional task, the skills needed for its execution, and the material conditions permitting optimal performance have been analyzed and even codified with respect to working conditions. It is now recognized that good interpreter training aims not only at teaching the techniques of simultaneous and consecutive interpretation, but also preparing the mind of the interpreter for cross-cultural communication. One need only think of the way Khrushchev used to flavor his speeches with Russian proverbs to appreciate the need for the interpreter to be sensitive to the subtleties of meaning in both cultures. The program for training conference interpreters at the Polytechnic of Central London, for example, is geared to developing a triple awareness: of the cultural and social mores that motivate the speaker; of how his speech can best be expressed by the interpreter without altering the message; and of the socially and culturally heterogeneous audience to whom the message must be clearly conveyed. On this last point, English is particularly sensitive, for it is the language to which many listen whose mother tongues are extremely diverse. For example, the interpreter may be called upon to render into English a speech whose subtleties are to be understood clearly by Japanese, Danish, and Pakistani listeners, as well as Americans and British. What else should be expected of the interpreter? An analytical mind, phenomenal short-term memory, tireless powers of concentration, and good health. To this list one might add the requirement for the right kind of psychological and physical makeup to permit sharing a tiny booth with another interpreter, sometimes for many hours on end, and the requirement to be able to lose one's own identity in order to play the role of the speaker being interpreted.

Of course there has been recognition of interpreting as an innate skill, and of the widespread phenomenon of natural translation, defined as "the bilingual translation done in everyday circumstances by people who have no special training for it." This condition is especially prevalent in bilingual countries like Canada and Belgium, where people from many walks of life, and of all ages, are frequently called upon to act informally as translators or interpreters. Studies have been made of very young children, under 3 years of age in some cases, who fall naturally into an interpreter role. In a different context, there is the

repeated phenomenon of a child acting as interpreter for another child whose speech is difficult for an adult to understand.

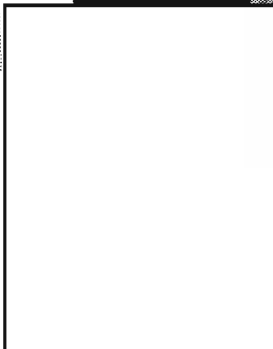
For many of those who are seeking to comprehend the nature of the linguistic process, the professional interpreter, engaged in either simultaneous or consecutive interpretation, has provided an ideal subject for research and speculation. Synchronous recordings of debates at international meetings and of their simultaneous interpretation have stimulated investigations leading to the detection of units of meaning, or chunks of language, contained in the listener's short-term memory. This unit of meaning can be defined as the smallest group of symbols required for making sense, the minimum for translating a message or a portion thereof. Some regard the translation act as consisting of two distinct processes: the translation of the input discourse into an internal cognitive representation, and the transformation of this representation into output discourse. Here again, the unit of meaning would play an important role.

Much of the research evidence suggests that the bilingual's two languages are learned as separate systems and function as such thereafter. This raises questions regarding the "switching" mechanism and how it functions. Relevant research also suggests that the bilingual's two linguistic systems feed into and draw from some common supralinguistic background which seems to be independent of any language. Far from resenting this intrusion into their mental processes, the interpreters seemed as interested as the psychologists in discovering how they do what they do so well.

Conference interpreting, which had started so informally, has now been institutionalized. Many of the old-time pros are refugees of one sort or another from World War II, who capitalized on their usually accidental knowledge of several languages. New entries into the field are a different breed, and are normally the product of one of a number of training institutions that prepare students for this specific application of linguistic skills. The market for conference interpreters is greatest in Europe, especially for Common Market activities in Brussels, and there are several excellent schools on the continent. There is one graduate-level institution in the United States that has a program designed to produce professional conference interpreters; the Monterey Institute of Foreign Studies. Courses are given there in Chinese, English, French, German, Russian, and Spanish.

It takes a special kind of person to be successful in the field of conference interpreting, and when one watches a highly skilled, experienced interpreter in action, it is an impressive display of how the human intelligence can be called upon for near-miracles of performance.

~~TOP SECRET UMBRA~~



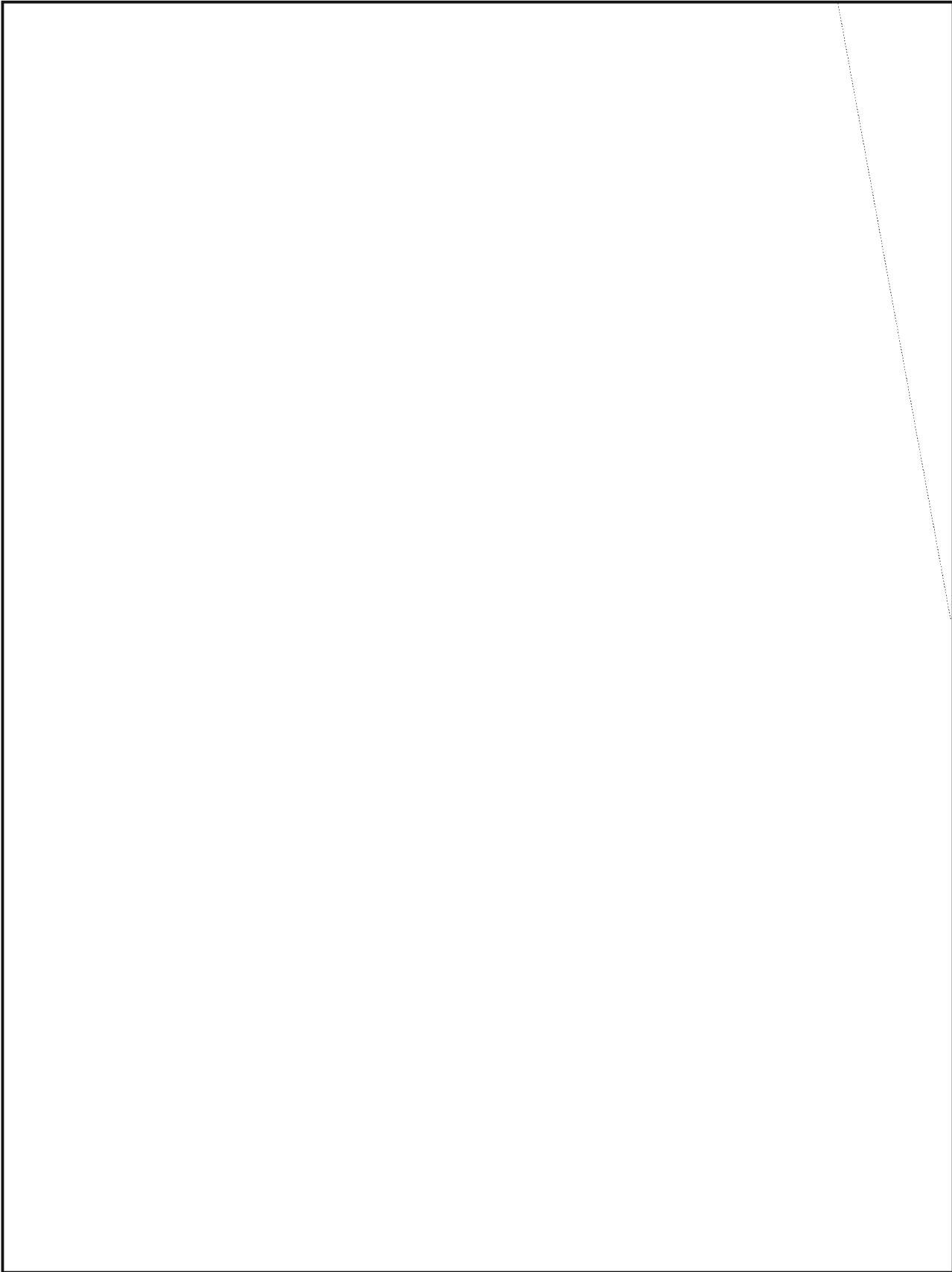
P.L. 86-36

*Reprint of A711 Informal
Technical Note 001-77*



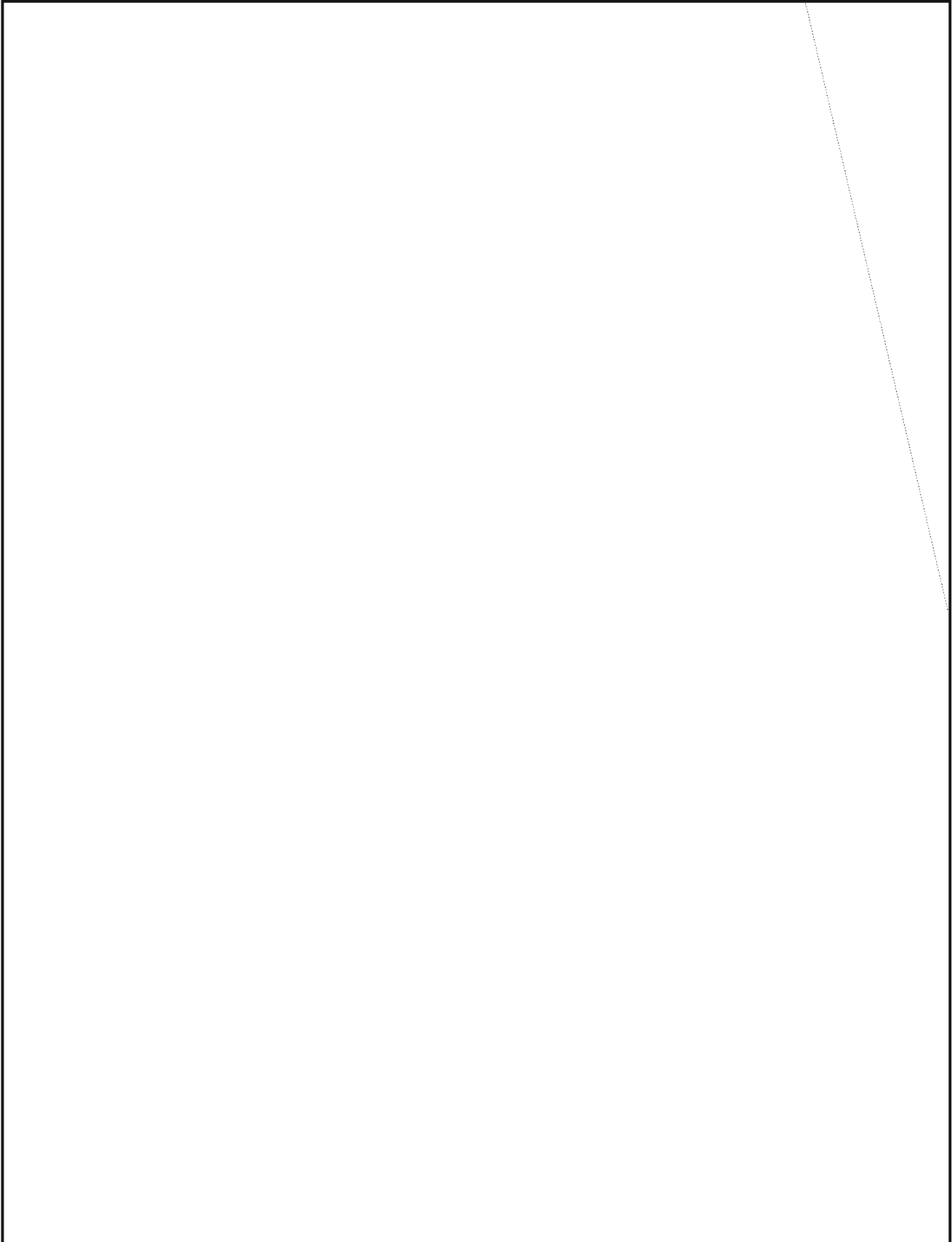
~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

First Lady of Naval Cryptology

RAYMOND P. SCHMIDT,
NSG Historian

Reprinted, with permission,
from the *NAVSECGRU Bulletin*.

Mrs. Agnes May (Meyer) Driscoll must have been a welcome person at Main Navy Building on Constitution Avenue in Washington, D.C. during the late 1920s and 1930s. She helped train Navy officers and civilians in the art of cryptanalysis (including the late Captain Laurance F. Safford, who first assumed direction of the "Research Desk" of the Code and Signal Section in OPNAV). After World War II, Mrs. Driscoll achieved recognition as a "principal cryptanalyst" for the Navy. She served in that capacity until December 1949, when she accepted a transfer to the Armed Forces Security Agency. She retired from active federal service on 31 July 1959.

Miss Agnes May Meyer entered the Naval Reserve in June 1918. In July 1919 she accepted a job as a stenographer for the Director of Naval Communications in the Code and Signal Section at \$1400 annual salary. Working up to the position of clerk by 1920, she subsequently resigned in 1923 to evaluate a new electric cipher machine for Mr. Edward Hebern. She "solved" a message in his "unbreakable cipher" and was on her way to becoming a code and cipher expert.

On 1 August 1924 Miss Meyer returned to the Department of the Navy; she never again left government employment until her retirement. A Government Accounting Office memorandum of 6 May 1925 shows her as a cryptanalyst earning \$1860 annually. In the mid-1930s she testified before the Senate Naval Affairs Committee that she had assisted the late William F. Gresham in developing a secure cipher machine for the Navy. The Senate appears to have believed her and awarded \$15,000 to her and Gresham's widow. Not only was she qualified as a cryptanalyst, but also she obviously had skill as a cryptographer.

Agnes Meyer had earned an undergraduate degree from Ohio State University in 1911. As a first-generation American citizen, she took obvious pride in her naval service during the "Great War." One of her personal data sheets lists special qualifications in physics, engineering mathematics, statistics, auditing, book-keeping, typing, and clerical work. She also possessed musical talent, having served as Director of Music in a small Texas school from 1912 to 1915. Then she became head of the mathe-



matics department of an Amarillo, Texas high school until enlisting in the Naval Reserve during the war. It is interesting to note that she qualified in four languages -- German, French, Latin, and Japanese.

Agnes Driscoll deserves recognition as a "plank owner" in the naval cryptologic organization. Her abilities and skills as a cryptologist were widely respected by several generations of naval and NSA colleagues. Although her technical contributions to the United States have not been reclaimed from historical records, they obviously deserve far more space than permitted in this article. It is characteristic of her cheerful modesty that she described her job simply as one involving "scientific duties."

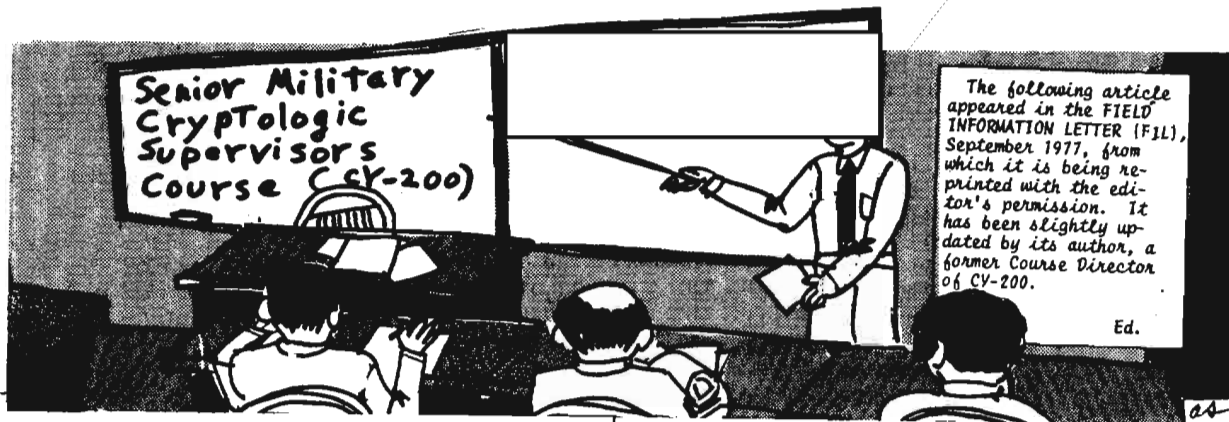
It would be sad, indeed, if Mrs. Agnes May Meyer Driscoll were to be forgotten by the present generation of cryptologists. We may very well owe her a professional debt that can only be repaid by continuing her rather awesome legacy of devotion and technical competence.

C.A.A. NEWS

The Communications Analysis Association's Winter Social was a great success, and why not? After all -- let's face it -- *free* parties are not that common around here. Of course, if you weren't a member, it did cost you something to get in. But *I* got in free and so did every other CAA member. Hope you got a chance to chat with the Director. (W.E.S.)

News from the CAA Special Interest Group on Cryptologic History: The group had its first meeting in November, and its first activity -- a tour of the P1 Cryptologic Collection -- in January. In December, members of the group received a copy of Dr. Harold Deutsch's article "The Historical Impact of Revealing the ULTRA Secret." Nonmembers of the group did not. Anyone -- CAA member or not -- who would like a copy can call Bill Nolte, 4087s, who can also explain the group's elaborate initiation rites. Future activities: In February or March (date to be announced): a session on oral history. (W.M.N.)

~~SECRET~~



Twice a year, the National Cryptologic School (NCS) conducts the Senior Military Cryptologic Supervisors Course, Course CY-200. This course is for the senior NCOs/petty officers and warrant officers who are "going places" -- that is, those middle-level managers who will eventually be moving into jobs requiring a wider range of cryptologic knowledge. The objectives of the course are to:

- increase the student's understanding of the relationships and functions of the cryptologic community within the national intelligence community and the U.S. government structure;
- demonstrate the impact of increased requirements, decreased resources, and increasingly sophisticated targets on the cryptologic community;
- illustrate the responsiveness of the cryptologic community to the National Command Authority in times of peace, crisis, and war;
- bring the student up to date on the latest developments in cryptologic technology, operations, policies, and plans; and
- further develop and prepare the student for positions of added responsibility by exposing him to a variety of subjects outside his own area of specialization.

CY-200 is open to personnel from all four military services, grades E-7 to W-4 inclusive. Additionally, the NCS may grant waivers for highly qualified E-6s. Students must have at least 8 years of cryptologic experience, preferably in operations (as opposed to maintenance, communications, personnel, and other support specialties). To insure maximum utilization after graduation, NSA policy is to give priority in selection to personnel in their thirteenth or fourteenth year of service.

The course lasts 7 weeks and is conducted at Friendship Annex (FANX). It is designed in modular fashion, with each module covering a

different subject area, as shown below in the schedule for Class 12 (summer of 1977):

<u>Module</u>	<u>Some of the topics covered</u>
Management Seminar	Contemporary management concepts, practices, and practical applications; problem-solving and decision-making; the planning and communicating process
U.S. Intelligence Community	Intelligence community organization and NSA's interface with it; role of the Director of Central Intelligence; Defense Intelligence Agency; Central Intelligence Agency; NSA support to national policy makers; national cryptologic security policy
SIGINT Resource Management System	National planning, programming, and budgeting; Consolidated Cryptologic Program; information management; economic analysis; resource management in the intelligence community; cryptologic planning
SIGINT Operational Process	

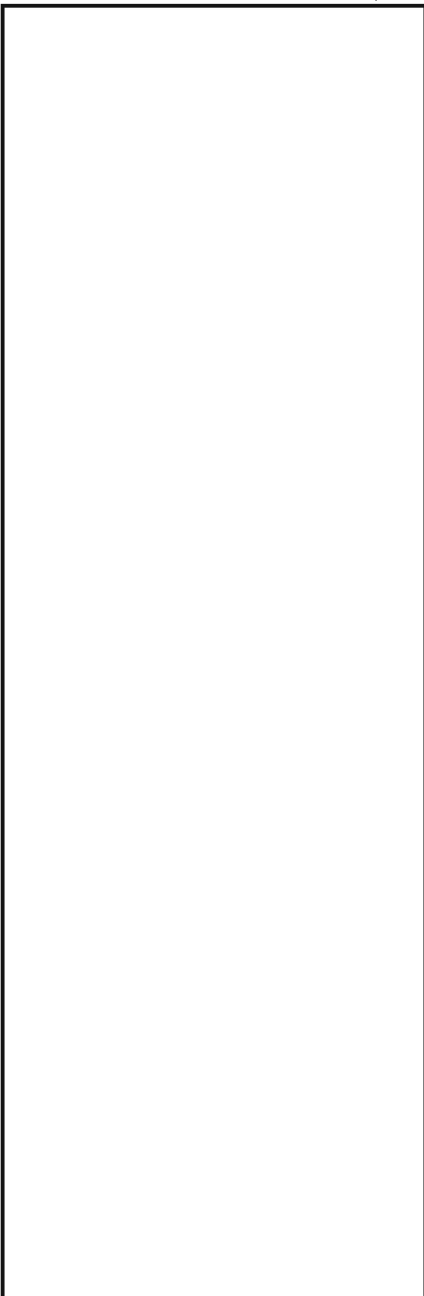
~~SECRET~~

HANDLE VIA COMINT CHANNELS ONLY

Support Activities and Area Studies

Role of the SCAs and SIGINT Support to Military Commanders

Communications Security



gives an introduction to the U.S. worldwide photographic-reconnaissance program. At NSA's Headquarters complex, students have the opportunity to tour various spaces, including NSOC, DEFSMAC, AROF, BROF, and GROF, various research and development projects, and COMSEC facilities.

Throughout the course, student participation is encouraged through the use of seminars, panel discussions, and student presentations. Students are able to talk to and interact with experts from many fields.

Senior officials of NSA/CSS and other agencies in the intelligence community regularly brief each class. SCA commanders and senior enlisted advisors are also frequent visitors to the CY-200 classroom. At the end of the course, students have seminars with the Commandant of the National Cryptologic School and Director, NSA/Chief, CSS.

Students are selected for CY-200 by a simple procedure. Three to four months before the next course begins, the National Cryptologic School sends course announcements to the military services and SCAs. The announcements give course dates and student quotas (class size is usually 45), and solicit nominees. The services then submit the names of persons nominated for attendance.

If you are interested in attending CY-200, contact the appropriate organization as indicated below, depending upon your branch of service:

<u>Service</u>	<u>Point of Contact</u>	<u>AUTOVON Number</u>
Army	MILPERCEN: (Enlisted: DAPC-EPL-M)	221-007. 10254/ 0329
	(Warrants: DAPC-OPW-AI)	221-7842
Navy	HQ NSGC (G131)	292-0757
Marine Corps	HQ Marine Corps (INT-S)	224-1208
Air Force	HQ USAFSS (DPXP)	945-2641

Since the first class in 1971, 316 students have been graduated from CY-200. Excellent comments on the value of the course have been received from the graduates to date. The distinguished graduates of the course include

[redacted] who is now the senior enlisted advisor to DIRNSA. So who knows what CY-200 will do for you? If you think that this course might further your military career and you would like more information about it, contact either the course director, [redacted] USAF, E61, on 8043s/796-6181, or the NCS Registrar's Office, on 8041s/796-6417. You're too late to be graduate No. 317 (Class 13 began in January), but there are still a lot of good numbers to come!

P.L. 86-36

P.L. 86-36

In addition to the lecture modules, the class also goes on a number of field trips. At the Pentagon, students visit the Defense Intelligence Agency, the National Military Intelligence Center, and the military services' operations centers, and receive briefings on the missions and functions of DIA and the Strategic Warning Staff. While touring the Central Intelligence Agency in Langley, Virginia, students learn about the CIA's role within the intelligence community, its SIGINT operations, and its production of intelligence for national-level customers. The class also makes a trip to the National Photographic Interpretation Center, where the NPIC staff

UNCLASSIFIED

MORE BEANS

NET WT. 16 OZS. (1 LB.)

Vera Ruth Filby, E41

Full text of all the papers presented at the ULTRA seminar will appear in a forthcoming issue of *Cryptologic Spectrum*.

We may as well get used to it -- used to hearing terms like "signal intelligence," "HFDF," and "traffic analysis" in public places, used to feeling exposed and unprotected at moments when our accustomed and familiar anonymity seems to be snatched away. Like most of us, no doubt, I had hoped that our "time of indecent exposure," as I have heard it expressed, might be nearly over, but a rainy October evening and foggy morning in Annapolis have persuaded me that we have seen only the beginning. Now that a few of our bean-counters' beans have been spilled, packs of hungry animals of various breeds, having caught the scent, are out there gnawing at the foundations of the storehouses, sniffing and rooting for more beans.

The occasion in Annapolis was the Third Naval History Symposium at the U. S. Naval Academy, 27-28 October 1977, specifically the Friday morning program on "Naval Intelligence in the Second World War." There, filling a tall, tiered lecture room in Rickover Hall, more than 200 people sat rapt for nearly 3 hours, without even a break, listening to presentations on "ULTRA and the Battle of the Atlantic." There it was easy to sense the appetite of the gathered historians for facts and more facts, their desire for truth and all the truth; and surely we can understand and appreciate that. The hunger -- even lust -- for information was evident even at the vast cocktail party the evening before, in the eagerness, for example, of a young historian snapping up a remark that there might be unreleased ULTRA information to be pursued. ("You mean," he asked, almost licking his chops, "there's lots more to come?") But influences other than scholarly questing for knowledge are present too, as I suddenly realized at the same party when an equally eager young historian, responding to a comment about inaccuracies in F. W. Winterbotham's *The ULTRA Secret*, retorted, "Yes, but it made him a million pounds."

Chairman of the Friday morning meeting was Harold C. Deutsch of the U.S. Army War College, and the speakers included:

- Patrick Beesly, former Deputy Chief, Submarine Plotting Room, the Admiralty;
- Jurgen Rohwer, Library of Contemporary History, Stuttgart;

- Kenneth A. Knowles, former Head, Atlantic Section, Combat Intelligence, COMINCH; and
- an unexpected bonus -- Vice-Admiral Sir Norman Denning, Naval Intelligence Division.

In his urbane and interesting introduction Dr. Deutsch remarked that many in the audience had been occupying themselves with the significance of ULTRA and said that although "tremendous euphoria" had followed the publication of *The ULTRA Secret* in 1974, savage reviews had sent the tendency in the other direction. (Incidentally, despite critics' attacks, there are some who, while deploring the publication of the book at all, consider the charges of technical incompetence too harsh. Winterbotham was not a technician and never said he was; he was the vastly experienced intelligence officer who served as liaison between the producers of Special Intelligence and the highest echelon of users.)

On introducing Commander Beesly, Dr. Deutsch showed advance copies of Beesly's book on *Very Special Intelligence*, being published in England and scheduled for publication in this country in March 1978. Commander Beesly opened his masterful presentation by defining terms. He pointed out that that the term the Admiralty always used was Special Intelligence, that there is almost no mention of ULTRA in British naval records, that ULTRA was a classification, not a cipher title, although the term has taken on that meaning as a result of the Winterbotham book. Commander Beesly said that it is impossible to overstate the value of SI, but he stressed that it was only one of many sources. The information from the triumphs at Bletchley Park went to the Operational Intelligence Centre (OIC), which was a "full and true" intelligence center. Even when most complete, SI needs the genius of a few experienced analysts to piece it all together. Even at its best, SI is useless if the users do not understand and accept it, and Commander Beesly told horror stories of events when commanders refused to accept SI conclusions. Both he and the following speaker provided extensive examples of the use of ULTRA results in protecting convoys against German submarines, and he noted that German operations against the east coast of the United States were detected in advance by OIC. He summarized the state of success

UNCLASSIFIED

at various phases of cipher recovery and the need during "blackouts" to fall back on HFDF (both he and the German speaker pronounced it "huffduff") and to try to read Admiral Doenitz' mind. Despite efforts at communications security, signaling remained necessary. U-boats had to report and to receive instructions, but later in the war the U-boat commanders were given more control and signaling became less frequent. At the time the Allies finally changed their codes in June 1943, both sides were reading each other's traffic without either being aware of the other's success. Concerning his sources for research on his book, Commander Beesly said that the British records were not complete but that many fascinating files were available from OIC and even from Bletchley. The most revealing were the weekly reports to the First Sea Lord, written by Beesly's chief, Captain Rodger Winn. The reports made by the tracking room were based mostly on SI. In estimating the value of SI, Commander Beesly said that its contribution was enormous in planning evasive routing and in concentrating naval forces, that without it victory would have come much later and at much greater human and material cost. SI, with the use of OIC and the U.S. Navy's OP-22-G made of it, was a war-winner -- but not the only one. The real heroes were those who risked their lives and often had to pay a fatal price for other people's mistakes.

After an enthusiastic ovation for Commander Beesly, Jurgen Rohwer continued the story from the German side. He began by noting that TV and the other public media have given the public the idea that the Allies knew every German move in advance. If that had been the case the Battle of the Atlantic would have been over much sooner. He explained that ENIGMA was the code-name for several cipher machines made by a private firm, and he described ENIGMA with slides showing rotors and other details. The German assumption was that the time needed to break an ENIGMA cipher would be so long that the results would be useless, and indeed the British did need the Polish and French reconstructions as a basis for their success. With a series of plotting charts on slides he showed the sequence of events at the time when both the Bletchley and B-Dienst cryptanalysts were reading each other's naval traffic and both sides were using radio intelligence, as he called it, in deploying and redeploying their submarines and convoys, in moves and counter-moves based on current decrypts. In evaluating the German use of ENIGMA, he said that there were mistakes, there was carelessness, that full use was not made of the machines' capabilities. By the end of the war, however, the German Navy was using up to 40 different ciphers, so that Bletchley had to set priorities for attacking and exploiting them. In summarizing the role of naval intelligence, he listed in priority order radio intelligence, DF, and traffic analysis. Radio in-

telligence had much greater influence on decisions on the Allied side than on the German. The turning point would not have come, as it did, in May 1943 without radio intelligence, and Normandy would have come much later. In a final, startling statement, he said the end might have come with the dropping of an atomic bomb on Berlin.

Dr. Rohwer's speech was a tour-de-force, and it too received a long ovation. It was an interesting experience to see these two representatives of the great opposing forces complementing each other's presentations and helping each other by pointing out the movements depicted on the slides.

An American followed -- Kenneth A. Knowles, wartime Head of Atlantic Intelligence, Chief of the Intelligence Staff of the 10th Fleet. Captain Knowles had come from his retirement home in Florida and had written his talk on his boat in Chesapeake Bay, depending entirely on his memory of events 35 years ago, without any recourse to official records. He opened by commenting that World War II had brought technical achievements of the highest order and that transcending all was the breaking of ULTRA. The Americans, he said, were more selective for need-to-know than the British, and only three persons actually dealt with ULTRA at Headquarters "in a former girls' school in Washington." At the communications center there, traffic included ULTRA results, HFDF telefax, and radio-fingerprinting reports. ULTRA results were, with one exception, never used without such backup as aircraft sightings, DF, or other cover sources. The one exception, the one risk taken, was against the U-boat "milk cows" in the South Atlantic, and the ULTRA-based action against them brought results, in Captain Winn's words, "too true to be good." The Allies recovered U-boat ciphers, grid location charts, and a new acoustic device. Historians, he said, have considered the turning point in the Battle of the Atlantic to be the summer of 1943, after the sinking of 90 U-boats. But the Germans were making technical improvements -- flash transmissions, an acoustic torpedo, 10-cm radar, new designs for U-boats -- so it was necessary to crush the Germans before these improvements began to have effect. In evaluating ULTRA, Captain Knowles pointed out that it was used for defensive as well as offensive operations. He judged that in its use the British were more clever and the Americans more daring, and said that the teamwork between them was superb. He commented on the value to cryptanalysts of the sheer volume of traffic stemming from Doenitz' insistence on direct control. No such volume would have been available without it, but then, he pointed out, Doenitz' methods almost worked.

The final speaker, not on the original program, was Sir Norman Denning, of British Naval Intelligence. In his opening remarks he made it clear that, although he did not condemn

UNCLASSIFIED

The ULTRA Secret, Winterbotham was the first person to break the oath of silence taken in 1940 when a select few signed their names to a document which forbade them ever to divulge ULTRA. He commented that surely ULTRA was the best kept secret in world history. He described early efforts to recover material to help in attacking the ciphers, the partial successes from, among other methods, capture of a weather ship, then recoveries from submarine U-110, after which Bletchley could read continental W/T traffic. But cryptanalysis is not the end of the job, he emphasized. Detailed analysis must follow; and he quoted from memory a comment referring to the World War I successes of Room 40, that "the information received has to be refined in the crucible of intellect and experience before it can be considered intelligence." In evaluating the results of SI, he said that only SCHARNHORST was a direct victim of its use. Sir Norman was in a reminiscent mood, and he spoke of Churchill in the anteroom of the war room just after the victory. "I see you're still celebrating," said the Prime Minister. "Can I join you?" And he turned to (then Commander) Denning and said, as Denning remembered it, "When I was a naval person we sometimes rang on the middle watch together in the dungeons of the Admiralty . . . You were the young officer who told me that total war required total intelligence, and without full commitment we might lose the war."

After more Churchill stories, the applause of the listeners demonstrated how fully they had entered into the mood of nostalgia he had evoked.

During the too-brief question time which followed, the questions showed the intense interest of the audience, an interest which is certain, it seems to me, not to slacken. Earlier in the program, Dr. Deutsch had announced that a TV program was being produced at the Army War College at Carlisle Barracks on the Battle of the Atlantic, to be made available to government agencies and perhaps the public, and he urged his Army and Air Force colleagues to do what they could to sponsor similar programs on ULTRA as it affected ground and air operations. The range of sponsors for the Navy conference -- including the Army War College, the Smithsonian, the National Archives, the Eisenhower Foundation, and the Naval Academy -- would suggest that more such conferences are altogether likely. This listener noted particularly the rather coy references to a certain "agency of the Department of Defense" which had been consulted about the symposium and the expressed hope that more information for scholars would be forthcoming. It is unmistakably evident that even military historians, who should understand the purposes of military security, will be exerting continuing pressure.

(U)

BY-LINES DON'T COST — THEY PAY!

JOHN J. MOLLIICK, B41

There has been a lot of talk recently about revamping procedures within the intelligence community to get bigger bangs from increasingly fewer bucks. That being the case, it appears the time has come to seriously consider instituting a relatively minor change in Agency reporting which I believe could greatly enhance the quality of our product, profoundly improve morale, and tremendously stimulate professional pride among the Agency's analysts and translators. And it wouldn't cost the National Security Agency one (pardon the expression) red cent!

My simple proposal is that NSA should begin putting the names of analysts and translators on the items they publish. This is no radical concept that has never been tried before. A number of sister agencies have long attached the names of their analysts to their products. As a matter of fact, by-lines on collateral items have several times served as my introduction to fellow analysts and have been responsible for my initiating mutually beneficial communications with those individuals.

Now that promotions seem to be farther and farther apart, new methods of increasing psychic income should be especially welcomed by those managers who are concerned with morale in their

organizations. As an analyst, I can think of no source of psychic income more rewarding than to see my name on a piece of intelligence I have done my best to produce. No analyst or translator worthy of the title can help but take increased pride in, and care with, his work if his name is there for the intelligence world to see.

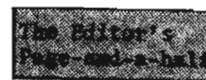
Within modern society as a whole, and certainly in modern government, there seems to be an increasingly dangerous tendency to shy away from fixing responsibility. Perhaps the most apparent truism of this age is the recognition that lack of responsibility breeds mediocrity. In addition to boosting morale, by-lines fix responsibility for the quality of our product. When names are attached to their work, professionals are bound to do their best all the time, and neophytes are compelled to improve rapidly by the most exacting of taskmasters -- their own developing reputations.

It is high time each analyst and translator is able to say to his peers, "This is my product. My name on it proves that I stand behind it. If it is accurate, don't hesitate to contact me, and perhaps we can help one another even more. If it contains error, tell me, and I'll try to improve. In any case, I proudly accept full responsibility for my work." The way to begin fixing responsibility, and giving credit where it is due, is by giving by-lines to live up to. The time to begin is now.

(FOUO)

UNCLASSIFIED

"NO, WINNIE, YOU'VE GOT IT UPSIDE-DOWN TOO!"



Whenever I make up an NSA-Croctic, I give an advance copy to the person whose published work I'm quoting from. I don't give any hint about who wrote it, and the person usually tells me what a surprise it was to have his own words jumping off the page at him. Therefore, when guest NSA-croctician David H. Williams asked me to preview NSA-Croctic No. 11, I was surprised to see the following text emerge:

[A. J.] Salemme, [*Guide to Russian*] *Technical Translation*, NSA, November, 1974, 189 pp. (U):

"The translator must . . . determine the precise type of [rotary-wing] aircraft . . . being referred to in Russian as . . . BEPTO Λ ET so that his rendition will conform to precise English usage. He must not . . . avoid the issue by translating it in formal context as 'eggbeater' or 'chopper.'"

All the time I was solving the puzzle, I was chortling at the way that Dave had used Latin letters in the WORDS to represent Russian letters in the word BEPTO Λ ET: the B in "This beets them all" suddenly turned into a Russian B (which is really pronounced V); the P in "Christopher Robin" turned into a Russian P (which is an R); etc. But what, I asked myself, was Dave going to do with the Λ ? The very last letter I put in the puzzle was in his "What f equals in a basic physics formula (3 wds)" -- "RECIPROCAL OF ___." I don't know from physics, so I said, "That son-of-a-gun must be using a Greek lambda!" so I

wrote in Λ in both places in the puzzle. When I phoned him and congratulated him on his tour-de-force, he said that my guess had been right: f (frequency) is indeed the reciprocal of Λ ([wave] length).

And so NSA-Croctic No. 11 was typed up for printing in the January issue. But, as is another practice of mine, I handed out some advance copies to a crew of people who like to do NSA-croctics critically, so that they can correct any typographical errors (178 instead of 187) or tighten up any definitions, etc. I was flabbergasted to learn that not one of them knew what to do with the letter in box 92. Here are the results:

<u>Previewer</u>	<u>"Words"</u>	<u>In text</u>
E.W., Russian linguist	"reciprocal of L"	BEPTOLET
	<u>Dialog:</u>	
	A.S.: "All the other letters are Cyrillic -- where'd you get the Latin L from?"	
	E.W.: "I thought of it as a Russian L, but wrote a Latin one."	
E.S., mathematician, knows "some Russian"	"reciprocal of F"	BEPTOFET
	<u>Dialog:</u>	
	E.S.: "The definition's wrong -- it should be ' f^{-1} '."	
	A.S.: "I don't know about that but I know that there isn't any Russian word with a Latin F in it."	
G.E., Mongolian linguist (Mongolian has lots of borrowings from Russian and an alphabet based on Russian)	"reciprocal of ?"	BEPTO ET
	<u>Dialog:</u>	
	A.S.: "What does the ? stand for?"	
	G.E.: "How do I know? It's a Russian word!"	
	A.S.: "Why didn't you look it up?"	
	G.E.: "I don't look up Russian words to do puzzles."	
T.L., mathematician	"reciprocal of ?"	BEPTOJET
	<u>Dialog:</u>	
	T.L.: "It's a Russian letter, but I don't know Russian."	
	A.S.: "Then where'd the J come from?"	
	T.L.: "I figured it was a kind of airplane."	

With this preliminary showing (four wrong answers from four smart people), I figured out that somewhat was awry with the puzzle. I asked Dave if I could edit it in such a way that any ordinary CRYPTOLOG reader (with no knowledge of Russian, or physics, or nothing!) could make his or her hand make the correct letter and then stick it in box 92. The thing I came up with was to shuffle some of the letters around and come up with a definition:

N O I S I A
119 44 182 164 63 92

(,,----- a,,)
sraeA 02 107 ahs head for 20 years
sas after standing on
what the Hindu holy man

Back to a new group of previewers!

<u>Previewer</u>	<u>"Words"</u>	<u>In text</u>
C.G.	NOISIA	BEPTO ET

Dialog:

A.S.: "Why is box 92 blank?"
C.G.: "Charlie [C.G.'s husband] says it's Russian, but the puzzle's 'too damned cute' for him."

G.T.	NOISIA	BEPTOVET
------	--------	----------

Dialog:

A.S.: "You had the V upside-down in the words -- why did you turn it right-side-up in box 92?"
G.T.: "I didn't know I could put it in upside-down."

A.S.d

NOISIA

BEPTO AET

Dialog:

A.S.: "Yippeel! You got it right! Why'd you put it in upside-down?"
A.S.d: "I figured it must be a Russian letter that looks like an upside-down V. But I don't know how to pronounce it."*

Having finally got one person with no knowledge of Russian (and no prompting from me) to write an upside-down V and place it in box 92 in that same attitude (is it coincidental that that person is my daughter Anne?), I figured that the puzzle was ready for the average CRYPTOLOG reader. With Dave's blessing and with E.S.'s fear that the definition might offend any Hindu holy men who might get to see the puzzle, we went to press.

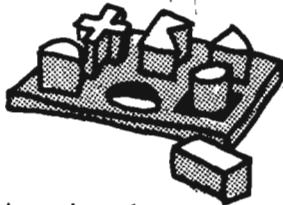
May I respectfully ask any CRYPTOLOG readers who did the puzzle, "What did you put in box 92? L? F? J? V? A? Or something else?" Or did you agree with Charlie, "It's too damned cute for me."

*Well, this is how you pronounce it. (First E is pronounced "ye" as in "yet"; second E is pronounced "yo" as in "yonder.")

B E P T O A E T
v y e r t o l y o t

Now say it -- "vyertoLYOT!" (Oops, I forgot to tell you to roll that R.) Try it again -- "vyer-r-r-rtoLYOT!" But you *still* don't know whether to translate it as "helicopter," "autogyro," "rotary-wing aircraft," "VTOL," or whatever. For guidance, see *Guide to Russian Technical Translation*.

PUZZLE



Getting back to that psychological test on page 1, where the cylindrical peg *does* fit into a square hole, here's a little puzzle you CRYPTOLOG readers can work on.

Assuming that one is allowed to use only solid figures (rather than squeezable ones) which have to fit completely contiguously inside the cut-out hole, one could pass several different objects through a two-inch hole in a board. For example, a two-inch sphere, a cylinder with a two-inch diameter, a cone with a two-inch base:



If you wanted to pass an object through *two* holes and have a completely contiguous fit each time, you could do that too. For example, if you had a board like the one shown below, you could pass a hemisphere through, holding it differently each time:



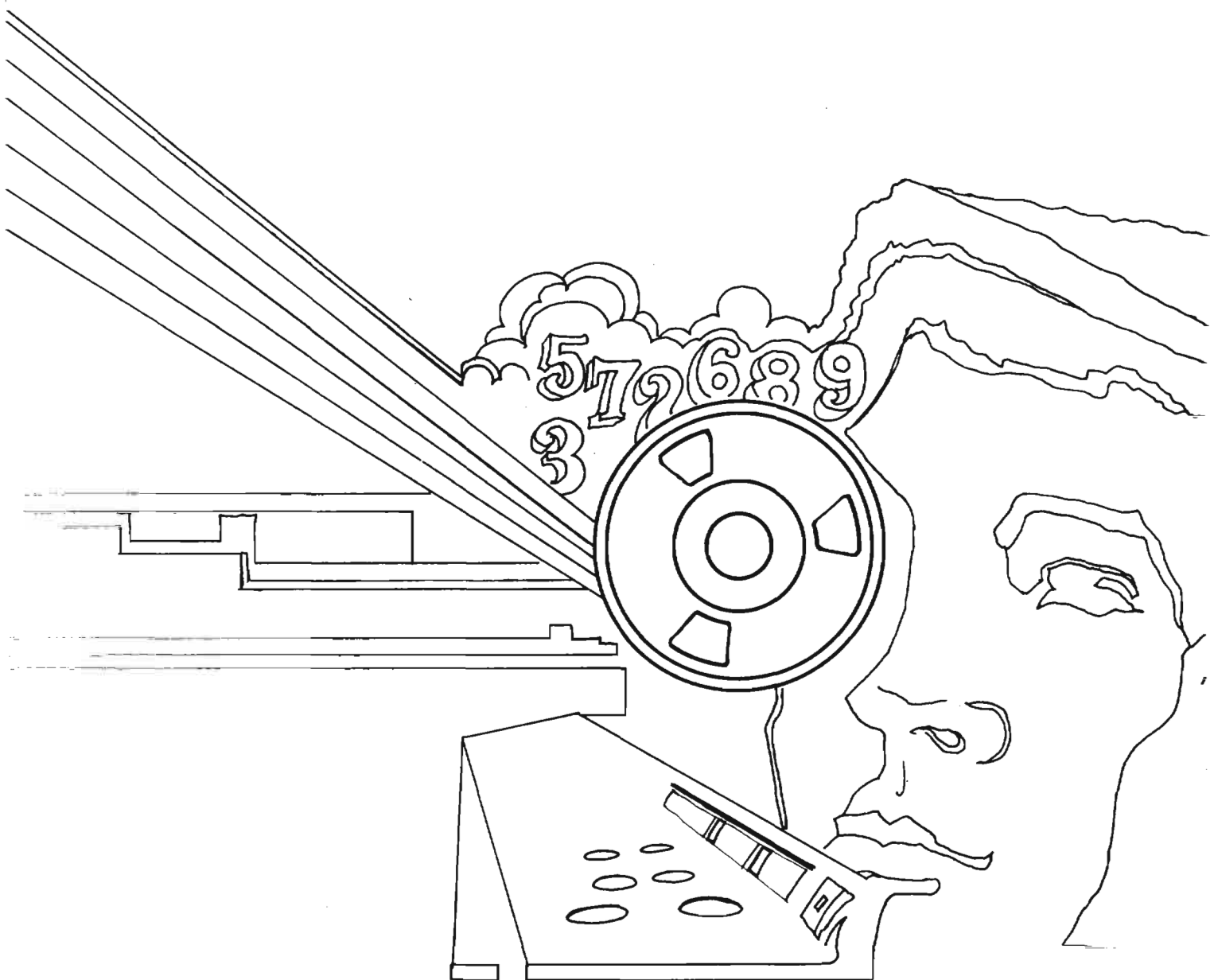
Now, then, the puzzle: Imagine a board like the one shown below. What *single object* can be passed through each of the three holes in turn, with a completely contiguous fit each time?



- 1 - 2" diameter
- 2 - 2" square
- 3 - 2" base, 2" height

A beautifully hand-crafted model of the object will be awarded to the first ten readers to send in the correct answer. (Answer will appear in next month's issue.)

~~TOP SECRET~~



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~