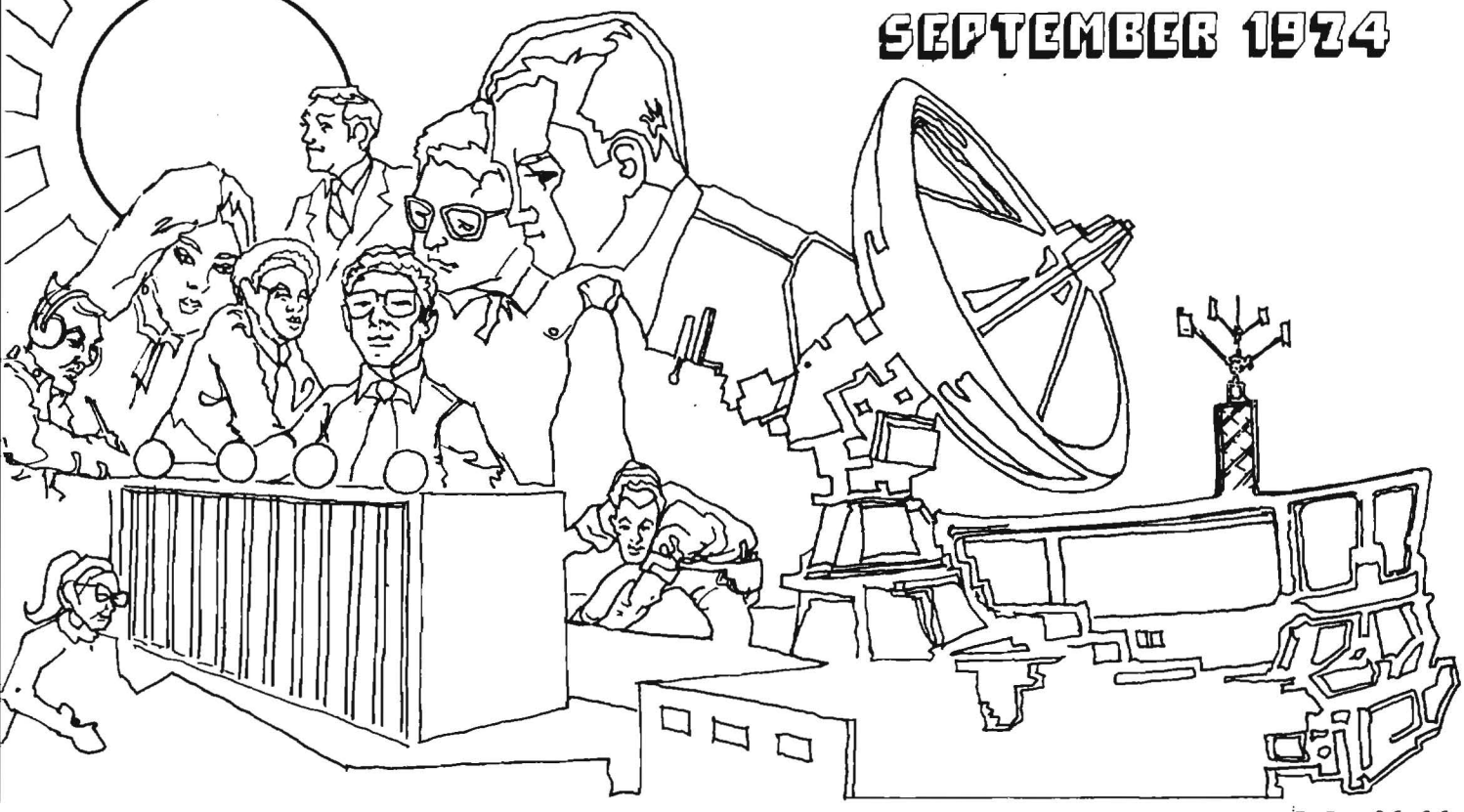
[redacted] TOP SECRET [redacted]

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

SEPTEMBER 1974



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

P.L. 86-36

[redacted] TOP SECRET

CRYPTOLOG

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

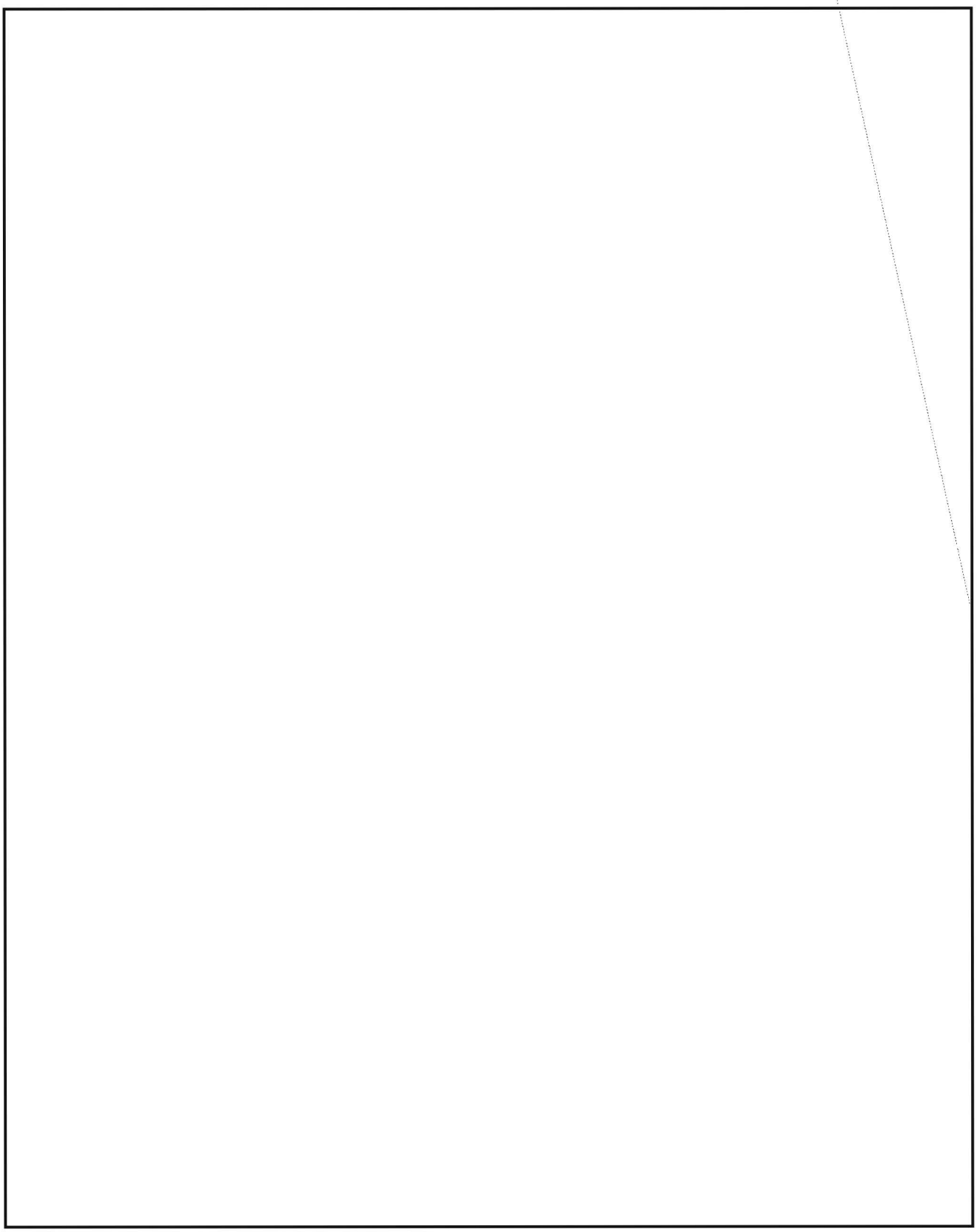
VOL.I, NO. 2 SEPTEMBER 1974

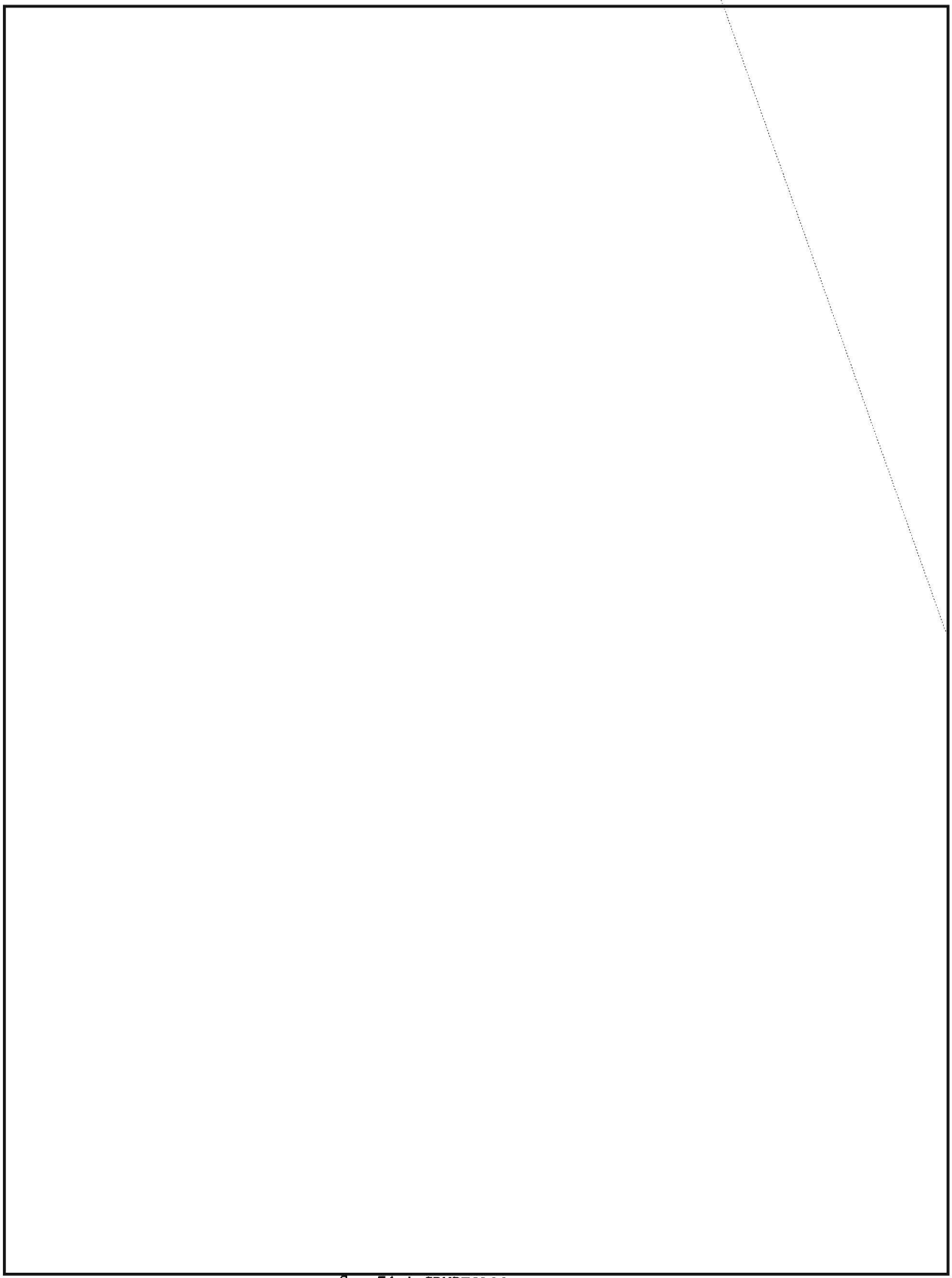
PUBLISHER WILLIAM LUTWINIAK

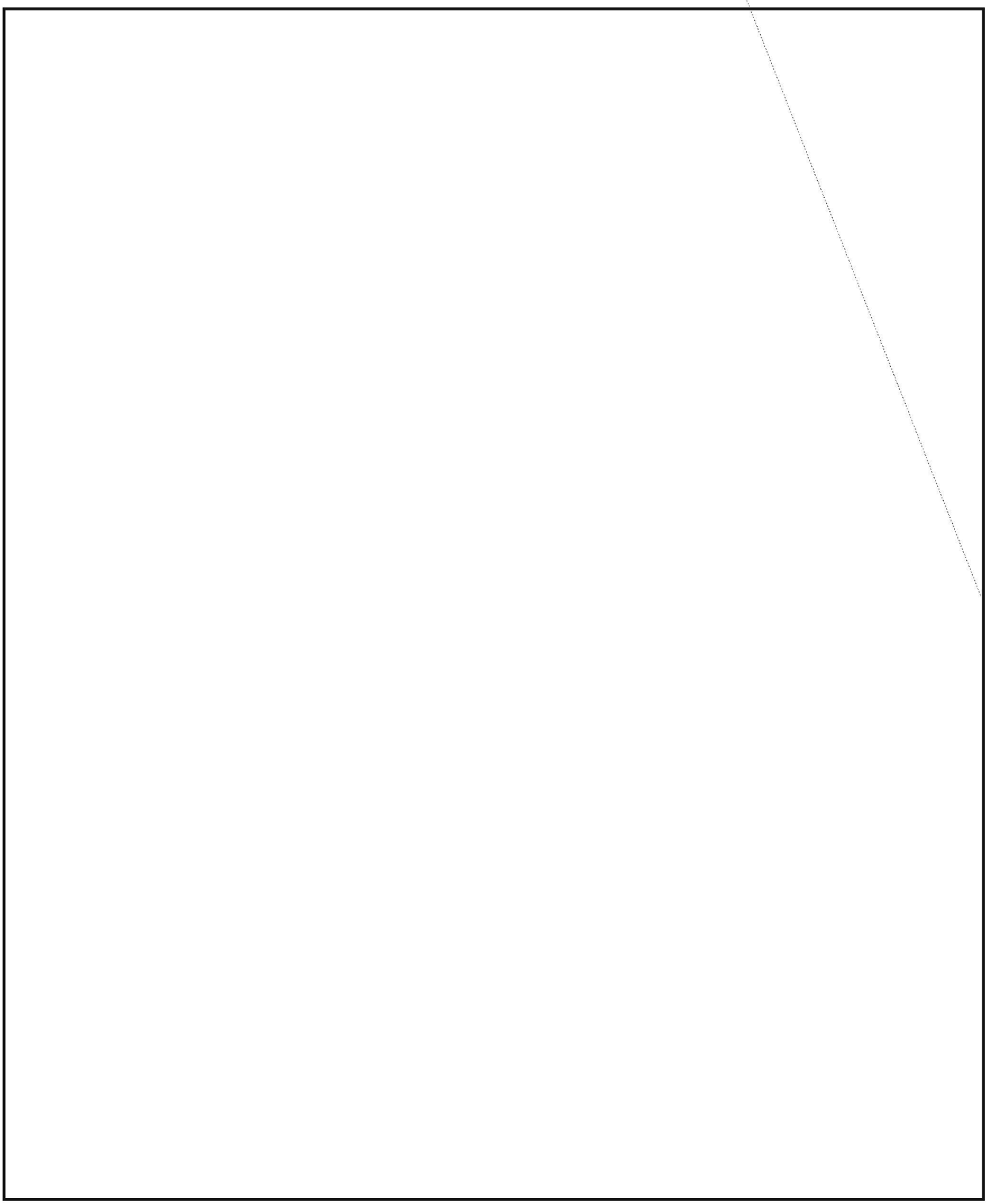
* * * * *

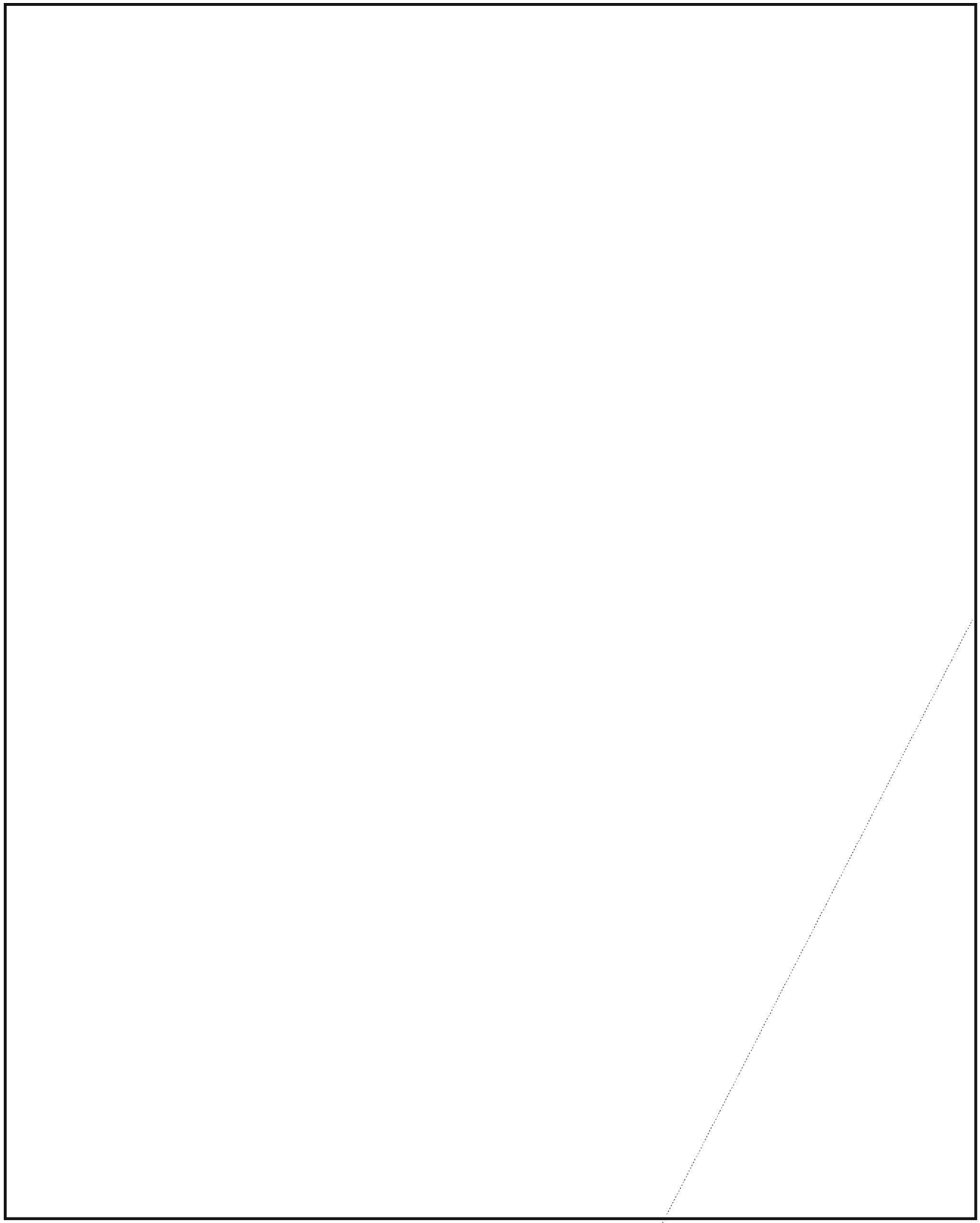
[redacted] TOP SECRET

~~TOP SECRET UMBRA~~





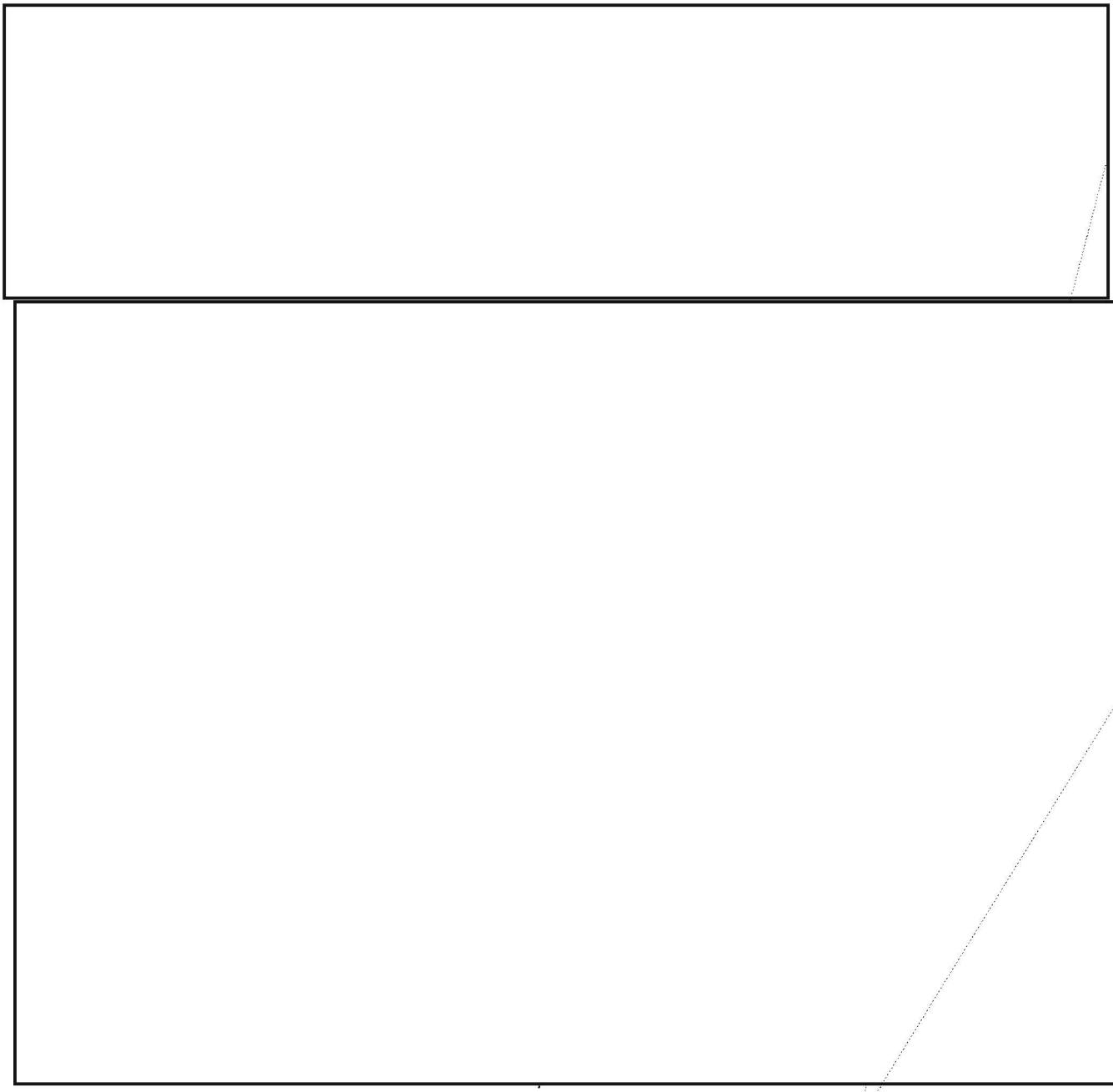


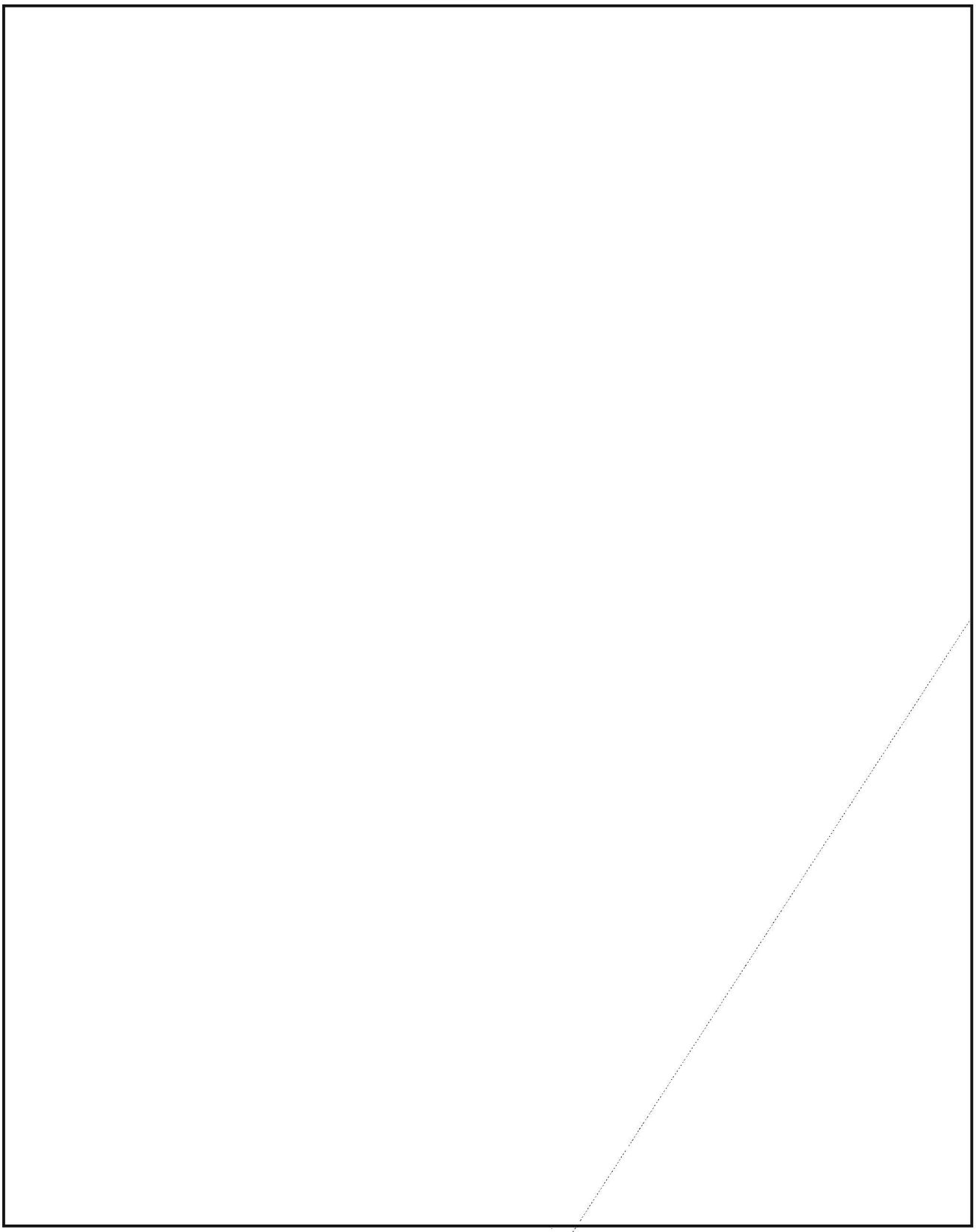


~~SECRET~~

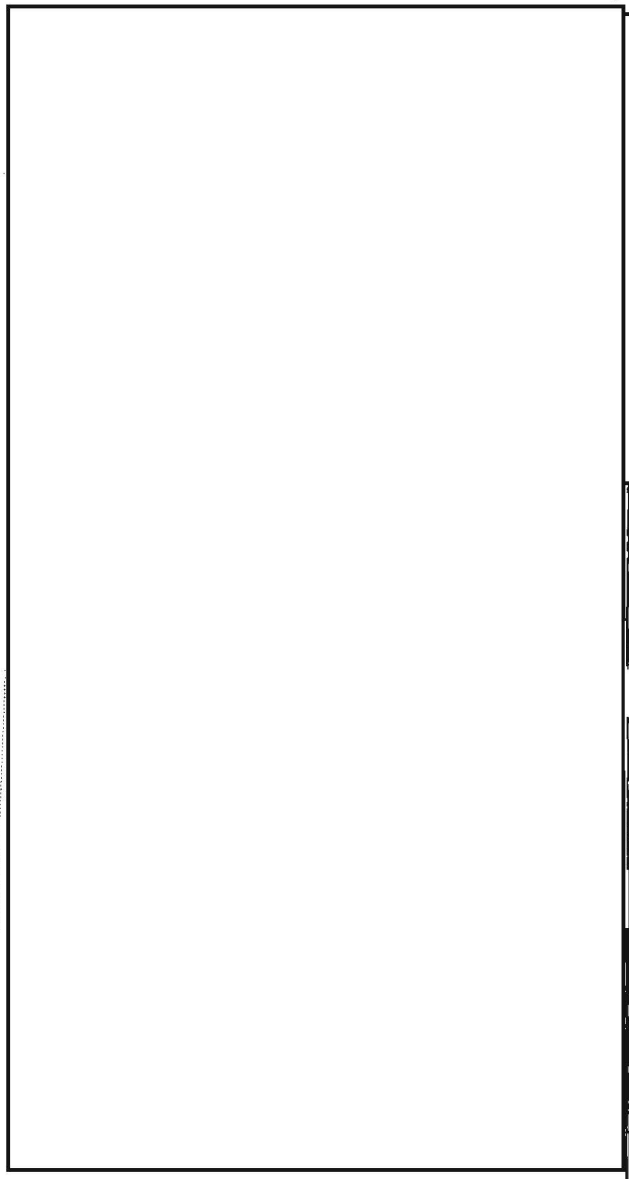
CRYPTANALYSIS & CODE RECOVERY

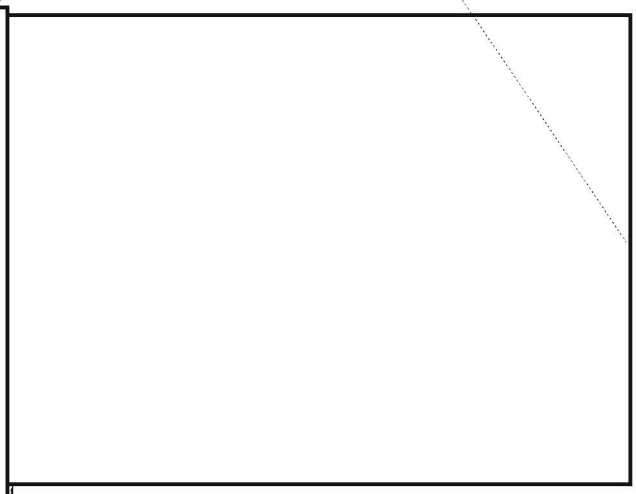
by MARJORIE MOUNTJOY





~~SECRET~~





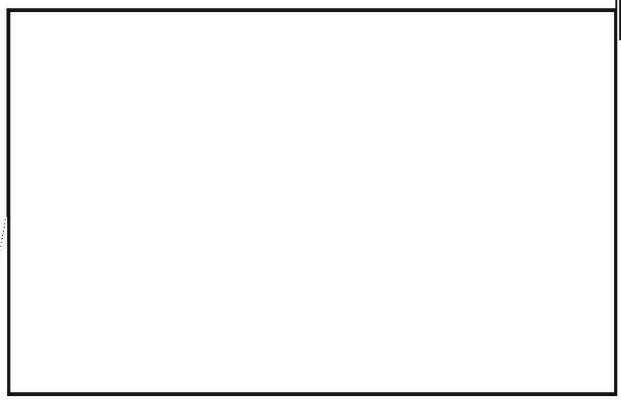
~~(SECRET/HVCCO)~~

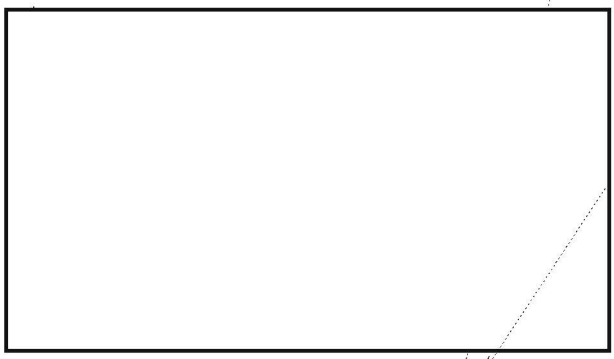
AS WE GO TO PRESS...

(A Note from the Collection Editor)

In a previous issue we explained that the raw material for analysis in NSA is not brought by the tooth fairy but is collected by units and people in the field. We are probably about to be given a graphic demonstration of how important those resources are.

* * *

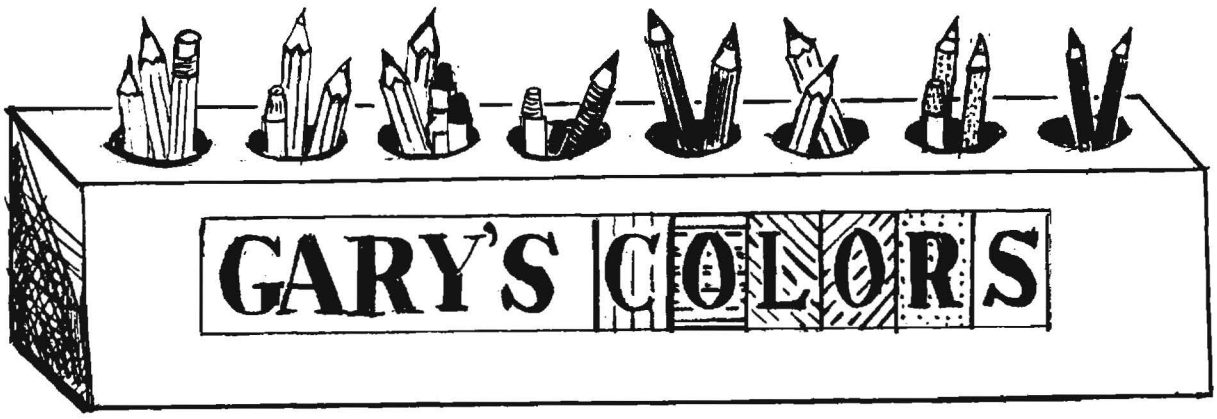




~~(SECRET/HVCCO)~~

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~



by Caterino G. Garofalo, P14

Frequently, studies in crypto-traffic analysis require differentiation in the quality of the data being researched. The use of a color scheme in recording the data facilitates such differentiation. I have developed and make use of one which is simple in nature and which my experience has demonstrated to be highly practical. The system uses the colors described below; they were chosen with specific purposes in mind. They permit the visual display of six different qualitative levels, which are also described below.

The colors:

Black - the black carbon #2 pencil has been found to be the best choice for normal usage, suitable both for erasure and longevity.

Green - is the weakest, that is, the lightest density. All of the other colors in the system superimpose on green quite readily.

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

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

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

I have found that colored pencils manufactured by different commercial firms vary considerably in hardness, density, and shade. It is desirable, therefore, having started with a particular brand, to continue with it and not intermix brands; this will ensure that distinctiveness and clarity are maintained. Also, once a color scheme is established for a given problem, maintenance of color discipline is mandatory in order to achieve unambiguous continuity of understanding of problem details regardless of changes of the personnel involved in the analytic effort.

The meanings of the colors in my system are as follows:

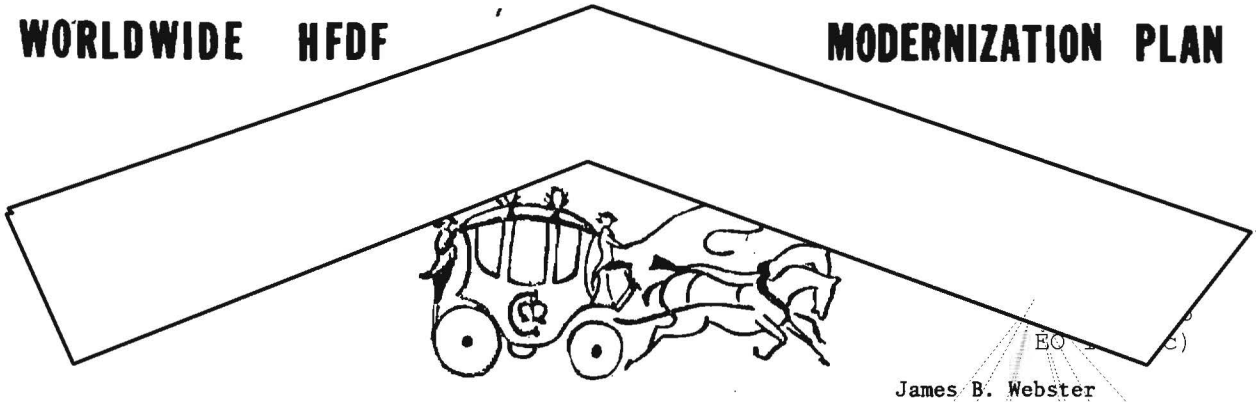
Color	Qualitative Level	Significance
Brown	5	The ultimate in degree of trueness; not to be questioned. May also represent captured or compromised information or its equivalent.
Purple	4	High in degree of reliability; may be used as a substitute or companion for brown where special conditions of clarity or distinction are vital to the problem. Primarily useful as a final and ordered value enjoying the same general stature as brown.
Blue	3	A relative base value having a significant bearing on the state of recovery.
Red	2	A base of lesser value or no relativeness (completely arbitrary); a necessary first step.
Black	1	To record or log information as it appears in its earliest or original form.
Green	0	Reserved for suspected garbles and for projected or expected but unobserved values (not proven but highly suspected as being correct). Used to alter a meaning or information without obliterating the original (black) form.

(UNCLASSIFIED)

This article originally appeared under the title "Simplicity in Color" in the October 1971 issue of COMMAND.

SECRET

WORLDWIDE HFDF MODERNIZATION PLAN



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

EO 1.4.(c)

James B. Webster

Reprinted by kind permission of the FIELD INFORMATION LETTER

Since the mid 1960's with the advent of the large Circular Disposed Antenna Array (CDAA) sites there has been a continued DOD effort to effect the consolidation and standardization of the US HFDF System. There is an inherent difficulty in consolidating these efforts,

These overall goals of DOD are being realized with the development of . Two programs, are the primary programs which will bring about this interoperable system.

Project is the overall plan to up-grade, modernize and integrate the existing worldwide HFDF facilities. It encompasses a number of the separate projects for improving individual facilities, specific service-upgrade programs and selected actions designed to integrate specific geographic networks. The primary goal of Project is to build an integrated national system to provide for the most modern, accurate and responsive HFDF system possible.

Project will also result in considerable manpower savings and some of these savings have been included in the fiscal planning for fiscal year 1977.

Project includes the following programs:

1. is the outgrowth of the U.S. Army and the U.S. Air Force Resource Change Proposals (RCP) designed to modernize and consolidate their respective HFDF systems.

The plan has a number of operational advantages in addition to manpower savings.

In addition, a common basis for training, procurement and maintenance is provided to the two services.

3. the U.S. Navy's project to modernize the Navy system. It includes automation of many functions now performed manually, thus resulting in extensive

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

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

SECRET

P.L. 86-36

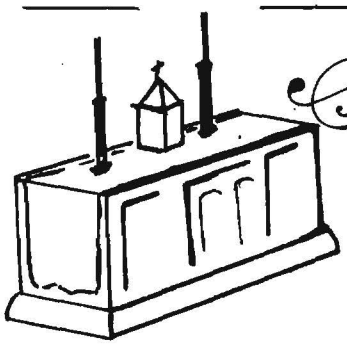
manpower savings. This is the largest of the projects [redacted] and is still in the design phase so that details will have to await a future publication.

[redacted]

The current plans are for completion of [redacted] in 1980 when [redacted] will be completed. The other projects are scheduled for earlier completion.

[redacted] is in the beginning stages of development. It presents many engineering and management challenges. As we proceed with its implementation, we will no doubt encounter many obstacles in engineering and operating this system. We feel certain, however, that [redacted] will go a long way toward meeting user requirements for increased numbers and accuracy of target locations.

~~(SECRET)~~



Secrets of the Altars: THE MOUSTIER CRYPTOGRAMS

[redacted]

Engraved in the stone fronts of two altars in a church in western Belgium are the Moustier Cryptograms--20 short lines of alphabetical text which no one has yet deciphered. Why are they of interest to Cryptolog? The answer to that question lies in an intriguing story that began in the first half of the last century and most recently included a request for help addressed to the Director, National Security Agency.

Professor Jean Connart, who is engaged in writing a history of the town of Moustier, has been trying since 1961 to discover the meaning of the texts. He has sought help from scholars, historians, archeologists, and military cryptologists--Belgian, French, Russian, German, American. All have been intrigued, but none has discovered the key to the cryptograms. The altar inscriptions still hold their secrets.

Early last year, Professor Connart obtained NSA's address from our embassy in Belgium and dispatched to the Director a plea for help. He enclosed photographs and a sketch of the inscriptions (reproduced at the end of this article) together with a number of substitutions he had tried and copies of responses to his similar pleas to others for expert help.

From those who have attempted to solve the puzzle come the following comments:

1. The texts contain a secret message (names of families, benefactors, etc.)

2. There are numerous digraphs (dipthongs) and doubled letters, perhaps represented by the "Greek" letters. (Disputed)

3. The job of the decrypter is to solve a substitution with multiple equivalents for some characters.

4. The underlying language may be Latin, French, Flemish, Spanish, or perhaps even English or German.

Professor Connart included some of his own notes on the history of the region, and these notes may have a bearing on the solution. According to parish records, the church at Moustier was in such dilapidated condition about 1836 that repairs were needed to prevent total ruin of the building. In addition, the winds of November 1836 had taken off part of the roof. In June 1838, some work was undertaken "in accordance with the plans of Philibert Pluvinage and Pierre Joseph Lemaitre. *A stonemason (un tailleur de pierre) received board and lodging for 18 days.*" (Italics Prof. Connart's)

(Continued on page 20)

LEXICOGRAPHIC CORNER

Some Thoughts on Lexicography

by Stuart H. Buck

Glancing through the latest bulletin of the Mongolia Society, my eye caught the following statement by John Krueger, professor of Altaic studies at Indiana University:

"The worst possible way to make a dictionary, and horribile dictu, the way that nearly all seem to be made, is to make a grand compilation of all existing dictionaries, possibly abridging slightly and adding a few examples. The obvious and ideal way, seldom followed, is to begin with a set of texts, draw from them only the words used in those texts, and create a dictionary out of the actual recorded usage of the literature (or in the case of a spoken dialect, from the noted speech of the speakers). The latter and better course is self-evidently vastly more difficult and time-consuming." [1]

These are the words of a purist. I must admit, however, that they really shook me up---not because I object, in principle, to definitions based on the personal experience and judgment of the lexicographer, but because Professor Krueger's "ideal" seems to me impractical, if not impossible to achieve (at least in a general dictionary). Now I have known John Krueger for almost twenty years, and I have the highest regard for his scholarship. I know also what he was driving at: the habit of so-called "circularity" among compilers of dictionaries, resulting in the perpetuation of ancient errors. Certainly this is a detestable practice, to be avoided if humanly possible. But where does one start? If Professor Krueger is so distrustful of others, where does he expect his lexicographer to acquire the knowledge of a foreign language which will be expert enough to enable him to read through both ancient and modern texts and to select from them the precise meaning of each word? When not reading, he is advised to glean terms from native speakers, presumably in the course of free conversations in their own language. Again, how does he acquire that skill? A modest amount of faith in someone else's judgment seems called for.

Part of the trouble, it seems to me, stems from confusing the role of the compiler of a general, or comprehensive, dictionary with the task of providing suitable "vocabulary lists" for a specific set of texts. Normally, this is the sort of information that the author of a reader provides in his glossary at the end of the book. To expect the lexicographer to wade, by himself, through all the published literature in a particular foreign language must assume that he would have the life expectancy of a Methuselah. Even then he would never quite catch up with the flood of new expressions appearing in the daily press. No, it is just plain unrealistic to expect the lexicographer to "go it alone!"

To be sure, it is flattering to view one's own products as truly independent, free of the slightest taint of plagiarism (that ugly word!). How nice

it would be if we could all operate in an ideal laboratory situation, with all the reference works we would like and quick access to native scholars (who are also bilingual)! All those knotty problems would fall like tenpins. Unfortunately, life is not like that---at least at NSA.

On TV we see the masked surgeon, garbed in his green gown and cap, working away in a germ-free room. There is a muttered command, a gloved hand is thrust out, and just the right instrument plops into it. Everything sterile, efficient, scientific, and prompt. Then we turn to old "Doc" in Gunsmoke, where someone is always getting shot up. No green gown here. The rule is very simple: The bullet has to come out! And Doc does it, rubbing his nose before and after the event. Somehow, his "patients" seem to survive.

Don't get me wrong. I'm not arguing for sloppiness--in lexicography or anything else. I'm merely saying that when there is a job of lexicography to be undertaken at NSA, we can either do it, honestly, as best we can or "leave the bullet in" and suffer the consequences. I heartily agree with John Krueger that there are good and bad ways to compile a dictionary, but I do not share his distaste for the eclectic method. The main thing here is to know your sources. Before you start harvesting words and examples from other dictionaries, find out all you can about each compiler---his background, purpose, method of operating, and reputation among his peers. Distinguish the sturdy oaks from the spindly saplings. I remember one work in particular that impressed me when I was compiling my Tibetan-English dictionary.(2) It was a massive tome, representing almost 50 years of careful research by several generations of conscientious French missionaries in the field.(3) These men were no dilettantes; they were dedicated to the task of spreading the gospel, and the Tibetan language was their means of doing this. Thus, their original word list was constantly tested, retested, corrected, and updated until they were finally satisfied that it was good enough to publish. One would be foolish indeed to ignore such a goldmine of information. The Chinese communists, who conquered Tibet, are also dedicated to a cause. They, too, are obsessed with getting a message across. Moreover, they have the enormous advantage of being on the spot, in control of the educational system. For anyone interested in understanding current Tibetan publications, the necessary clues are to be found in Chinese cribs---or in the special glossaries that accompany translations of Marxist texts. One could spend a lifetime plowing through the Kanjur and Tanjur (i.e., the sacred literature of Old Tibet) and end up incapable of reading editorials---or even telegrams---in this new, ersatz Tibetan.

On the other hand, the lexicographer is bound to run into dictionaries, glossaries, or private files of dubious value. Again, the tipoff is to know something about the author. Was he a "language bum" making quick trips in and out of one language after another? Or was he only interested in one subject: e.g., mathematics, zoology, botany, religion, entomology, ichthyology, folklore, etc.? Where did he get his information? By asking "informants" whose knowledge of English was minimal or who were so anxious to please that they would agree immediately with all his conclusions? I know of one lexicographer who regarded camel drivers as a prime source of information. Well, if camel drivers are anything like truck drivers, I wouldn't put it past them to take a malicious delight in pulling the leg of an inquisitive foreigner.

Now let me get one thing straight: I am unalterably opposed to the notion of a general dictionary as a "dumping ground" for every card file, glossary, or dictionary in sight. I believe that lexicography is primarily a process of

selecting or rejecting information contained in all available lexicographical sources, plus the author's own experience in the language. At this point I agree completely with Professor Krueger that the lexicographer should read extensively in the target language, selecting words, phrases, and examples of usage as he goes along, with special care taken to record the precise source of everything extracted. If challenged, he should be able to say, "That's where I got it. You take a look and tell me what you think!"

It pains me to bring this up, but I think it not unreasonable to assume that the lexicographer is well enough versed in the other language to check his own ideas in native dictionaries. It is one thing to base everything on what a lot of foreigners have said that a particular word means. It might be quite revealing to discover how natives define the same term in their own tongue.

Above all, it is imperative for the lexicographer to know exactly what he is trying to do. Don't leap on your horse and ride off in all directions. Ask yourself, "Why am I compiling this dictionary?" "Who is going to use it---and for what purpose?" "Will it meet the specific needs of NSA linguists?" "Is this the most practical format to follow in order to achieve my stated aim?" Are you trying to please some entrenched clique or other because you are afraid of hostile criticism? If so, you had better forget the whole thing because you are bound to be clobbered by someone---and perhaps unfairly. Life is like that!

You can take your lumps if you believe in what you are doing and give it your very best effort. Remember that you will never have enough time to do as good a job as you would like. Inevitably, your published dictionary will contain mistakes, but don't be dismayed. There will be plenty of kindly souls around to point them out to you. If it turns out that you are wrong, admit it---and thank the person who spotted the error. Also, make sure that an errata list is distributed to all users of the dictionary, under your name. This is vitally important because I insist that the lexicographer must stand back of his product, personally. He can select useful information from any source, but he must form a value judgment on each item selected---and answer for it. This does not guarantee that he will be infallible, but it will keep him honest.

I hope that no one gets the impression that I think that a large, general dictionary should be compiled by one person, single-handed. That is almost too much to expect of mere mortals. The eclectic method, which I support, does not require that all contributors be dead. Considering the magnitude of the task, a joint effort is highly desirable---so long as someone assumes responsibility for the overall product. Also, there is no great virtue in trying to do everything by hand. Make an imaginative use of the computer. Think of it, however, not as an insatiable monster requiring constant feeding, but as a faithful servant who will save you an enormous amount of labor.

(1) The Mongolia Society Bulletin, Vol. XII, Nos. 1-2, 1973, page 53.
(2) Buck, Stuart H., Tibetan-English Dictionary with Supplement, the Catholic University of America Press, Washington, D.C., 1969.
(3) Les Missionnaires Catholique du Thibet, Dictionnaire Thibétain-Latin-Français, Hongkong, 1899.

UNCLASSIFIED

LANGUAGE IN THE NEWS

by P16

P.L. 86-36

It's quite possible that some of our readers have missed the following items. CRYPTOLOG accordingly relays them as a public service to NSA linguists.

AFRIKAANS: The Union of South Africa recently banned its first Afrikaans book. Government censors had previously banned many books in English but never had occasion to suppress works in Afrikaans, usually because people who wrote in that Dutch-related language stuck to traditional themes or topics approved by the government. However, Andre Brink recently wrote a book called KENNIS VAN DIE AAND (Knowledge of the Night) about a black actor's love for a white girl, his attempts to establish a theater with a message for black people, his torture at the hands of security police, and his conviction for murder. Some people describe the book as "trash" and "evil" while others compare it to Solzhenitsyn's exposes of Stalinist repression. Brink is working on an English translation so you may soon have a chance to judge for yourself.

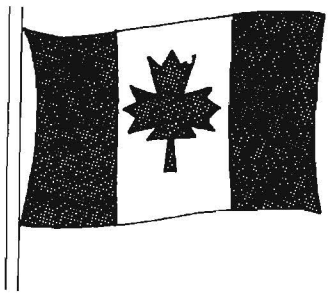
AMERICAN INDIAN LANGUAGES: The Wisconsin Native American Languages Project is an undertaking funded by the Great Lakes Inter-Tribal Council, Inc., to involve speakers of Wisconsin Indian languages (Ojibwa, Potawatomi, Menomini, and Oneida) in the application of linguistics to the analysis, study, and teaching of native American languages.

ARABIC: Is becoming one of the official languages of the United Nations (along with Chinese, English, French, Russian, & Spanish) because several Arab states agreed to meet the entire cost of expenses entailed in installing additional sound booths in all conference rooms and channels for interpreters and the hiring of additional personnel -- $8,300,000 for the next three years.

CHINESE: The government of Hong Kong recently passed a bill making Cantonese Chinese an official language of the Crown Colony, alongside English. Now leaders are busy trying to draw up programs to improve the standards of the language spoken and to get the government to use simple Chinese in its communications with the public (avoiding esoteric and outmoded terms). It has also been suggested that Mandarin should be declared equal in status with Cantonese.

官話

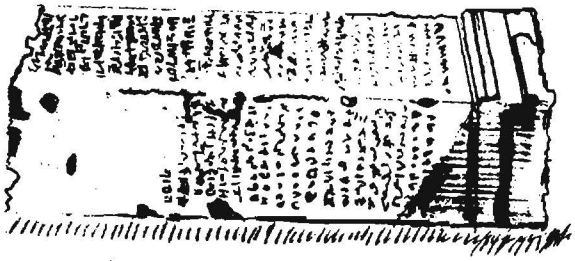
FRENCH: The government of Quebec, after years of controversy and debate, finally proclaimed French the official language of the province. Of Canada's 22 million people, 6 million speak French (5 million in Quebec and the rest in the other 9 provinces). Despite government emphasis that Quebec's 13% English-speaking minority's rights would be respected, many people worried about having their children forced into French-speaking schools. The matter became an issue in last July's election, which bilingual Pierre Eliot Trudeau won.



The French-speaking people of Switzerland's Jura region, after 159 years of trying, finally won a battle for separation from the predominantly German-speaking canton of Bern. The Jura, along the northern border with France, had been attached to the canton of Bern in 1815, but by a surprisingly close vote (36,802 to 34,057) the Jurassiens voted in favor of making Jura Switzerland's 23d canton and the sixth with a French majority. The capital of the new canton will be Delemont.

HEBREW: Many of the babies born in Israel during and right after the October 1973 war were given names connected with the war fronts and Yom Kippur, the day on which hostilities began. Thus, there will be a new crop of Israelis bearing names such as Golan, Golana, Sinai, Sinaya, and Miah (from the initials of the phrase MILCHEMET YOM HADIN, War of the Day of Judgment). Since the cease-fire brought about by the shuttle diplomacy of the US Secretary of State, a number of newborn Israeli baby boys have been named Henry Kissinger Cohen, Henry Kissinger Goldberg, etc.

LYCIAN: An archeological team recently unearthed a 4-foot, 4-faced limestone tablet in southern Turkey with inscriptions in Lycian, Aramaic, and Greek. Scientists have compared the find to the Rosetta Stone because with it they may be able to unlock the mysteries of Lycian, an Indo-European language spoken in southwestern Asia Minor back in the 5th and 4th centuries BC.

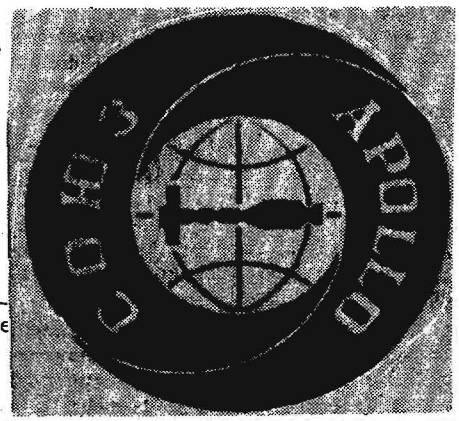


POLISH: When Archbishop Agostino Casaroli, Vatican Secretary of State, went to Warsaw to confer with the Polish Foreign Minister, it led to speculation that diplomatic relations may soon be resumed. The Archbishop even spoke some Polish while there. "Let God guard Poland and lead it to great and happy goals," he said, adding "NIECH ZYJE POLSKA!" ("Long live Poland!")

SPANISH: Mexico City's mayor thought "it was getting so one couldn't tell whether one was in Mexico or Manhattan" so he banned English-language commercial signs in an area visited largely by American tourists. The mayor might have experienced the same disorientation of locale had he toured Manhattan's Spanish-speaking upper East Side.

SPANISH AND PORTUGUESE: The Library of Congress recently issued a document entitled Latin America, Spain and Portugal: An Annotated Bibliography of Paperback Books, a list of 1,512 inexpensive paperbacks currently available. It supersedes an earlier (1967) bibliography that was restricted to Latin American works and includes travel guides, grammars, readers, dictionaries, and textbooks (Spanish & Portuguese). The cost is a mere 75¢ and you can order it from the Superintendent of Documents, Washington, DC, 20402.

RUSSIAN: The emblem chosen for the patch to be worn by the astronauts participating in the joint US-Soviet space mission in 1975 will include Cyrillic lettering. The Russian word SOYUZ (union, unity) will appear on it, along with the English word APOLLO. The mission names will encircle a drawing of the two spacecraft docked together above the world.



SWAHILI: Kajiga Balibutu, a priest in the African country of Zaire (formerly the Belgian Congo), recently completed and published a 700-page Swahili dictionary. Unfortunately, the report from Azap (the Zairese news agency) didn't specify whether the work was a bilingual dictionary or was entirely in Swahili, but our guess is the latter.

A LONG HARD LOOK AT THE Intern Program

by 'Anne Exinterne'

In 1965 NSA started an Intern Program designed, according to the Personnel Management Manual, "to provide the quantity and quality of professional personnel required to perform effectively the professional work functions of the Agency." The PPM further states:

> "An intern program provides the mechanism through which an annual input of pre-professional personnel with appropriate qualifications will be broadly trained in line with current and projected needs of the Agency as well as the participants' immediate and long-range career goals. The goal of each intern program is to assure that high-quality pre-professionals are carefully selected, initially trained, and given a proper variety of job assignments to prepare them for filling professional positions in a particular career field."

In view of the budget cuts that the Agency has taken in recent years and the resultant restrictions in hiring, a Special Task Force was appointed last year to study the intern program and to recommend whether it should or should not be continued. While I would not disagree with their recommendations that it should be continued, I would recommend certain changes on the basis of my experience as an intern and graduate.

Promulgation of Program Philosophy

I do not believe that many of the interns or line supervisors are aware of the intern program philosophy as it is stated in the PMM. In fact, I had never read that description before I began this paper, and I doubt that the recruiters who interviewed me and some of my contemporaries had read it.

The version that we heard went something like this: "Most of the Agency's top managers will be eligible for retirement in the early 70's. The Intern Program was created when the Agency realized that bright young people would be needed to fill the gaps left by these retirements."

Now, not even in our naive and brash youth did many of us imagine that managers from Dr. Tordella on down would anoint us to be their successors, but it did seem that we were going to be groomed for great things; and some of the first interns accordingly dubbed themselves "FSG's": "Future Super-Grades."

It was not too long, however, before hints of reality began to creep into this rose-colored picture. For one thing, if this was to be a management-training program, where were the management courses? Most panels do not require any management courses; some include one; and none, so far as I know, make an attempt to include on-the-job training in management. For another thing, while the panels have often referred to interns as a "select" group, as does the PMM description, their sheer numbers discount claims of much selectivity: to date, over fifteen hundred interns have entered the program.

I concluded some time ago that the real purpose of the program was to train new hires of average or slightly above-average potential to be competent technically in one of the Agency's career fields. I say "average or slightly above" because the admission requirements of most of the panels require a Staten score of 5 in the appropriate CQB (Career Qualification Battery) category. Such a score indicates what the Personal Management Manual describes as "average test performance" and would place that person in the middle of a bell-curve distribution of test scores. (As a predictor of success in that field, it indicates that the person has approximately a 55 percent chance of performing above the average for a total test group composed of all NSA employees and applicants.) If I had a lot of faith in CQB scores as predictors of success and did view the intern program as a highly selective one, I would require a Staten of 7 in the appropriate category, indicating that the candidate's performance was "distinctly above average" and that he had scored better than 84 percent of the people taking the test.

It seems that the PMM statement about the program's supplying input to career fields "based on current and projected needs" was not taken very seriously by the panels or by the operational elements. If it had been, would the Agency now be faced with the current skill imbalance? Some of the operational elements tended to use the intern program as a "billet savings bank" which could be added to or taken from as other needs dictated. Since then, direct control over those billets has been taken from them. Unfortunately, however, it appears that panels are still being encouraged to supply graduates for fields currently over strength. The Study Group which reviewed the program last year recommended that "interns currently in the program /who are/ training for skills that are in excess in the new TD be immediately evalu-

ated by ADPS for redirection to other career fields where vacancies exist." Instead of redirecting interns in such programs, M3 is continuing to recruit new hires for overstrength fields, on the theory that "every field needs new blood." How will these new hires react to the knowledge that they are being trained for a field in which the Agency already has a surplus of personnel and that they may be without a billet when they graduate, or that after spending three years in training for one field they may be asked to retrain in another?

After nine years of program operation, it is time to make sure that recruiters, supervisors, interns and panel members have a common and realistic picture of the program philosophy.

Recruitment

If I were recruiting for NSA I would, first of all, recruit high school graduates for many of the jobs now identified for college graduates. There are many jobs at NSA which involve very routine procedures, and in the past there has been a tendency to use college graduates for some of these jobs. The philosophy behind this may have been that they would be more alert to new techniques that could be used, but I suspect it was more likely the result of the now-fading obsession with hiring college graduates for all jobs. But just as the outside world has come to appreciate the importance of the trade and technical school graduate, the Agency shows signs of beginning to appreciate the high school graduate. It is time to take a close look at some of our jobs and determine exactly how complex the duties are and what type of educational background really is needed.

As far as college graduates are concerned, where there are people already trained on the outside, I would hire those people rather than trying to create a data systems analyst out of a psychology major, and I would not try to fashion an Arabic linguist out of an English major until I had checked to see if some of the linguists that Uncle Sam had trained and then turned loose were interested in Agency employment. Nor would I hire a person because he had a specific skill and then give him an option to use or not to use that skill. A friend of mine scored straight 7's on a scale of 9 on the Russian test, but when she came on board she was given a choice of several internships and selected Data Systems; a military convertee who had been trained in two scarce-skill languages at Uncle Sam's expense entered the Special Research Program. I don't mean to imply that if you are hired in one field you should be required to spend the next 30 years in that field, but I think you should at least be initially assigned to a position that makes use of your background.

(A note on military personnel who wish to convert: I have known a number of such people who had a sincere interest in converting but were reluctant to try because of the polygraph. Since the polygraph is forbidding even to people like me who were raised in a rather protected pre-drug, pre-coed-dorm environment, and have backgrounds that could probably be checked out in an afternoon, it is not surprising that men and women who have been in the military and who have not been in such a protected environment should have considerably more qualms about it. Other than drugs and sex, a major problem seems to concern the discussion of classified material. Although supergrades can be heard discussing such material in the halls--and if the tables at the "602" could talk, KGB agents would probably feel guilty about collecting their checks--civilians, with but rare exceptions, do not have to face the polygraph again. However, the enlisted man who wants to convert knows that he will be asked something to the effect, "Did you ever divulge classified information?" While he knows that he has not divulged it to unauthorized persons, he also knows that his mind will go back to conversations in the NCO club in Turkey or the NSA cafeteria that M5 would not have endorsed, and suspects that he will react to the question. I think that M5 must be realistic in dealing with such people, as compared with college hires who have only been exposed to classified material via James Bond. Perhaps they are realistic--but the potential convertees do not know that, so some elect not even to try to convert.)

Related subject: I suspect that the testing battery and other screening devices used by M may be producing a population that is too homogeneous. Well-rounded people are good company, but people with a bias in one direction often provide the spark that "all round good fellows" cannot. Does it really matter if a superb linguist almost did not graduate because of trouble with math? Or that a computer whiz would never pass a Dale Carnegie course? Or that a first-rate signals analyst has problems with grammar and a girl in every port?

Admittedly we cannot have thousands of brilliant but querulous technicians, but there must be a middle ground, and this is where personality and aptitude tests could be put to better use. It would be worthwhile, for instance, to give the Minnesota Multiphasic Personality Inventory, the Kuder Occupational Preference Test, and others, to a hundred outstanding crypt-analysts, traffic analysts, linguists, etc.; there is a very good chance that personality patterns associated each profession would emerge. The Agency relies heavily on aptitude tests, but the fact that a person scored well on the language aptitude test does not necessarily mean that he will be a good transcriber--that he has the temperament that will enable him to sit at a position eight hours a day with earphones on.

Such tests would be especially helpful in evaluting liberal arts graduates. I am told that in the early years of the program about one college recruit in five expressed an interest in personnel work -- usually because he was disenchanted with his assigned field. Naturally Personnel cannot absorb all those interested. I do not think this disenchantment with the technical side of NSA is unusual or surprising considering the number of liberal arts graduates with no directly related skills who are recruited. Many of the people who came in with me had majored in English, History, Political Science, Psychology and Sociology, and had a bent of mind that is not needed or even useful here. To me and my friends, for instance, numbers that show attrition rates by college major would be fascinating, whereas numbers that show a station's frequency usage for the month would not. It is true that we can cultivate an interest in this, just as we can learn to take frequency counts, but the traffic analyst or the cryptanalyst needs a special insight or interest that we do not have, and the Agency would be better off training someone whose natural bent is in that direction.

The recruiter who interviewed me made a rather feeble attempt to see if I had the type of personality required for CA work by asking if I liked crossword puzzles. "Sure!" was my enthusiastic reply. Much later, when I really thought about that question and understood why it was asked, I realized that I hadn't worked a crossword puzzle since the eighth grade, but I wasn't consciously lying when I gave that answer; I think you will find that a recent college graduate who is jobless has an open-minded interest in almost anything that seems to interest the interviewer.

If he had asked, "When was the last time you worked a crossword puzzle from start to finish?" and "Have you ever tried to figure out what was wrong with the family radio when it didn't work?" he might have gotten a closer indication of where I would--and more important --where I would not fit in at NSA. The Agency could devise a preference test to determine what interests applicants have that might suggest an adaptability for NSA professions (e.g., "Rank the following subjects in the order in which you would prefer to take them: Translation, Math, English, Philosophy, Psychology, Programming, Music, Sociology").

It would also be helpful to ask the potential employees what they think they might be doing at NSA, based on knowledge of the Agency they have acquired through open-source publications, etc. Like many recruits I had a mistaken notion of what I might do at the Agency. I thought I would probably be researching and preparing biographies on foreign personalities. After hearing my idea (had he asked) the recruiter probably would have been wise to refer me to CIA.

In some ways the recent budget cuts almost have a bright side so far as recruiting is concerned. The Agency no longer needs droves of new employees. As result there is no reason why an applicant should be hired who is not exactly the type of person we want and need. The number of college seniors taking the Professional Qualification Test, the Agency's first screening tool, was still high the last time I heard, the job market is tight, and NSA offers a good starting salary, so there is no reason why we should settle for second choices.

(Next issue: Selection and Orientation)

(UNCLASSIFIED)

* * * * * * * *

AN EDITORIAL NOTE:

We in NSA have had too little discussion--in print--of controversial issues, and it is easy to see why. In the world at large the writer on serious questions works with considerable freedom. Subject only to his conscience and the demands of truth, he can hew to the line and let the chips fall where they may. In NSA, however, we are a closed community; the "line" runs close to home, and the chips inevitably fall on our colleagues, our chiefs, ourselves.

This is a great inhibitor of comment and correction. If it were only possible (we have all thought at some time) to discuss the problem apart from the people! But even if I am willing to take the consequences of my words, and the icy wind that may thereafter blow from the front office, it will look as if I'm getting at Phil or Liz, and I don't want that at all.

To alleviate this situation, CRYPTOLOG invites informed and thoughtful discussions of current issues, with or without an author's pseudonym. (As explained on page 21, and as required by all serious publications, the writer must identify himself to the editor, but may request anonymity in print.)

So give your country the benefit of your views!

DEPARTMENT OF GOLDEN OLDIES

King Eusyb & Queen Deodi

(c. 1961) [redacted] P.L. 86-36

Once upon a time there was a rich and generous king named Eusyb, who dwelt in a tower of purest ivory. He had one weakness--an inordinate craving for rich pastries of all sorts, but especially for dark brown devil's-food cake with thick fudge frosting, which he demanded every Friday morning promptly at 0830 hours (with occasional samples on other days); and he insisted that some always be available in the event that unexpected visitors should call.

Queen Deodi handled the funds, and she was very frugal. The royal baker, Durensi, found it most difficult to stay within the budget because of King Eusyb's weakness. He sent his assistants to faraway lands to obtain the exotic materials needed for these confections, and some of them were so closely held by their owners that they could not be purchased at any price. But Durensi and his assistants were faithful servants and they frequently obtained the needed goodies by stealth. The scarcest commodity was cocoa, which was needed to produce King Eusyb's favorite, that dark brown devil's food cake. Unfortunately, the entire world's production was controlled by the wicked King of the North, Ivan the Awful, who jealously guarded his shipments, and disguised the cocoa beans in every possible way. He went to such lengths that Durensi and his men would sometimes find a single bean hidden in a whole wagonload of garbage.

So Durensi's assistants started intercepting all the garbage shipments they could find and sending them home to their own land to be sifted through; and all went well until Deodi got wind of the project. She was very wroth, and told poor Durensi that he must not waste his funds in this way or she would reduce his budget. Durensi explained that he was only searching for cocoa beans to prepare King Eusyb's favorite dish, and the Queen finally relented. However, she told Durensi that he must not keep so much garbage in the royal castle, and that his assistants must sift it as close as possible to the point of intercept, sending home only the goodies which they found.

Durensi complied, but he was sorely troubled. He had spent a long time and had invested much money in equipment and training; now he was fearful lest he lose technical continuity, forget how to sort garbage, and lose the assistants he had trained to run the complicated sifters, sorters, slicers, dicers and ricers. He explained the predicament to his staff, who made the following recommendations: (1) Move the bakery farther away from Deodi's chambers, (2) use some of the garbage which had been closely associated with cocoa beans as a cocoa substitute when there was not enough of the real thing available, (3) convince the Queen that the men in faraway places did not have the equipment or the technical ability to extract the goodies from the garbage, and (4) demonstrate to King Eusyb that, by noting the type and quantity of garbage collected, the time and place of collection, the direction of travel and mode of transportation, it would be possible to keep tabs on the disposition of King Ivan's cocoa caravans.

Durensi was persuasive, and before long all these things were done. A new bakery was erected, far from Deodi's chambers, hidden in the wilderness where only the most loyal and dedicated assistants were willing to travel. Fresh garbage began to arrive and soon the vast storage and processing areas were full to overflowing.

But Deodi became very upset as Durensi hired more and more assistants. She suspected that much of the sifting was not producing any goodies, and was being done only to keep the helpers on the payroll. So Durensi hit upon another scheme: he would get a superduper sifter/sorter/slicer/dicer/ricer which would sift, sort, slice, dice, and rice a hundred times as much, automatically, as all his manual sifters, sorters, etc., were capable of doing. This would not only produce more cocoa beans, it would reduce the tremendous backlog of garbage and prevent its building up in the future.

King Eusyb, with visions of devil's-food cake with thick fudge frosting dancing in his head, heartily endorsed the plan. Deodi, too, was delighted, seeing not only an opportunity to get rid of the accumulated garbage but also to reduce the number of manual sifter, sorters, slicers, dicers, and ricers in the bakery. But just when it seemed that Durensi's troubles were over, he suddenly found himself worse off than ever. Queen Deodi told him that he could not hire and train people to operate the new

equipment because he already had more assistants than he really needed. At the same time King Eusyb would tolerate no lag in the production of devil's-food cake.

More garbage kept flowing in. In desperation Durensi took some of his more experienced workers off their jobs to train on the new equipment. It was not enough. The new equipment required more and more workers as it approached the operational stage. This cut deeper and deeper into current production, and the garbage collected faster than ever. One day Durensi and all of his helpers were smothered under an avalanche of garbage.

Not long afterward, unexpected visitors arrived at the castle. They were King Ivan the Awful and his warriors. Just as they approached, Queen Deodi was murmuring comfortably to her husband, "You know, dear, our budget has certainly stretched a lot further since we got rid of Durensi and his smelly crew."

(UNCLASSIFIED)

(from p. 10)

Secrets of the Altars

In spite of these repairs, the church was (c.1840?) in such poor condition that part of it collapsed when the roof was raised. The contractors had to rebuild the choir and the side chapels (where the altars are) from the ground up.

There is a published report (Moulart, *Basecles; Esquisse religieuse)* that the ancient altar of St. Martin was sold or offered for sale at Basecles in 1843. Basecles, a Belgian town near the French border, contains the Church of St. Martin which dates from 1779 and is considered the best product of the Tournai School. Does the Moustier St. Martin's altar come from Basecles? Were both it and the Virgin's altar constructed in 1843? Or does only the stonecutting date from that time? Answers to these questions could have a bearing on the date of the Moustier cryptograms and their underlying message.

Like to try your hand at this puzzle? Send your proposed solution to the Editor who will pass it on to the Oglethorpe Team which handles such problems for the Agency. Cryptolog hopes to publish in a future issue an article about the workings of that group, which some of us have heard of and some have not.

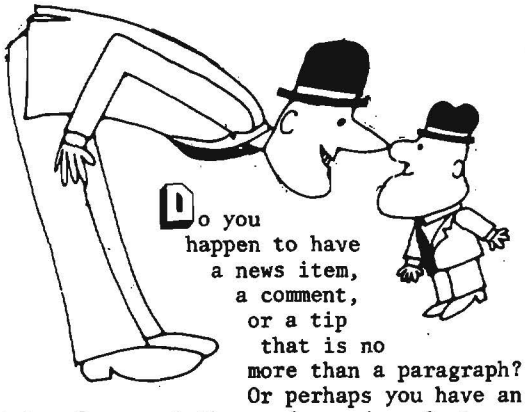
Meanwhile, here are the inscriptions. Good Luck!

(UNCLASSIFIED)

St. Martin's Altar

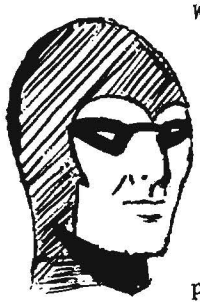
The Virgin's Altar

Contributions Solicited



Do you happen to have a news item, a comment, or a tip that is no more than a paragraph? Or perhaps you have an article of several thousands words...? Long or short, if it has something worthwhile to say, we'll print it. (For your interest and guidance, one page of typescript, double-spaced, makes about one column in CRYPTOLOG.)

First-person articles or stories about your own experiences are welcome, so long as they relate to our work. (See "Busman's Holiday" in the August issue.)



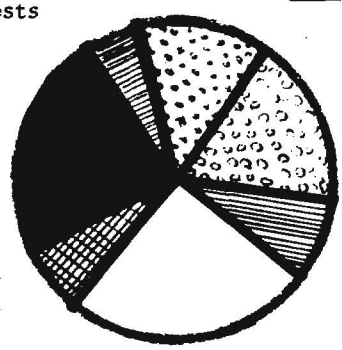
Want anonymity? A thoughtful piece on a subject of interest to many readers will be considered for anonymous publication, if the writer requests it. (The writer must, however, identify himself to the editor in an accompanying note or by a personal call.) Needless to say, personal or trivial complaints will not be considered.

Photographic illustrations can be reproduced, at the same quality as those in the NSA Newsletter.

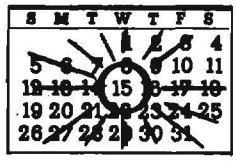
Sensitive materials? No. We'll go all the way to Top Secret Codeword, but we have to draw the line at compartmented or otherwise exlusive sources.

Your contribution does not have to be typed; we'll give preference to content over form, every time. (Though, especially in the case of a long piece, the editorial eye will appreciate any effort you can make in that direction--garbles and strikeovers freely forgiven.)

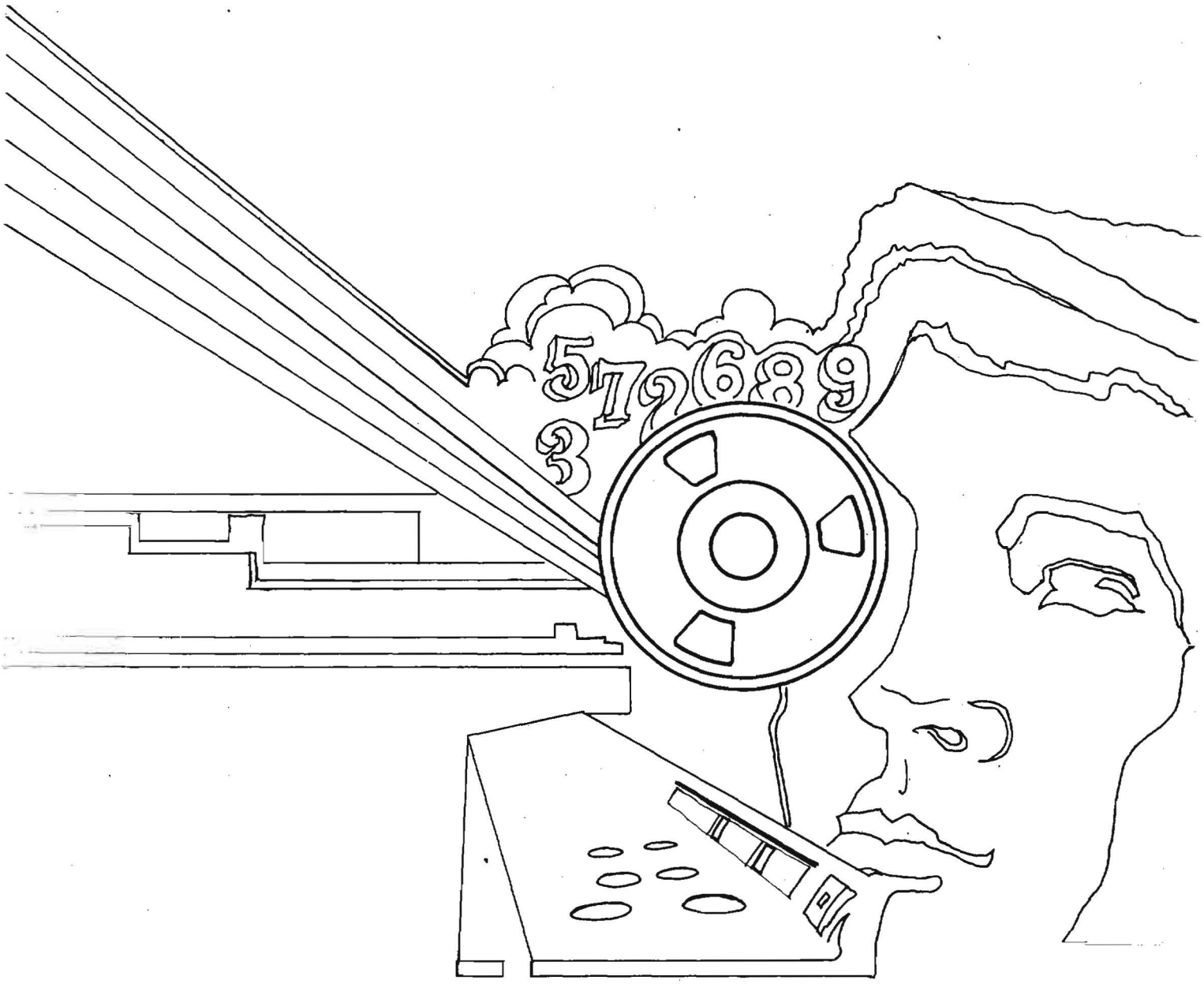
Something missing? If you feel that your work or your interests are not being well represented in CRYPTOLOG, it's probably because you and your friends are not contributing. The editors earnestly want to cover the whole territory, but articles don't grow on trees, y'know! Somebody (who knows the subject matter) has to write them.



Need assistance? You may have an idea, or some notes, or even a half-finished paper that you feel has possibilities but you don't quite know what to do with. A call to the appropriate departmental editor will get you a "story conference" and possibly inspire you to finish it up and get it into print.



Our deadline is theoretically the middle of the month (the 15th of August, for publication in October, and so on), but don't let that stop you if something good comes along on the 16th. And anyhow, this is a monthly publication; if you miss this month's deadline you'll be just in time for next month's CRYPTOLOG. See you!


5 7 2 6 8 9
3