~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JULY 1977

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

VOL. IV, NO. 7 JULY 1977

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

~~TOP SECRET~~

THE TRANSCRIPTION SKILL: CONCEPTS AND TEACHING METHODOLOGIES

P.L. 86-36

ACKNOWLEDGEMENTS

The author owes a great deal to her students for their suggestions, which have helped to improve the quality of the transcription course and which have made the classroom activities more effective.

She also wishes to express her gratitude to her many colleagues for their cooperation in answering the questionnaires which provided much of the foundation of the paper, to [redacted] *for their valuable suggestions, and to her supervisor, Harvey Hoffman, for his encouragement and support.*

A special debt of gratitude is owed to [redacted] *for his thoughtful assistance, in both the development and preparation of this manuscript.*

N. B.

The National Cryptologic School (NCS) is currently offering many transcription courses to develop students' ability to listen to recorded tapes and transcribe them. Since the transcription skill is not one of the so-called four skills involved in foreign-language learning (listening, speaking, reading, writing), it appears that no academic institutions have offered courses specifically to develop this skill. Moreover, little research has been done on this subject. Consequently, teachers at NCS are individually experimenting with various methodologies to teach the transcription skill. For these reasons, there is a need to clarify and establish a definition for the skill of transcription, identify the relationship between the skill and the other four skills, describe the level of the transcription skill which the students should attain, and develop an effective methodology to use in teaching the transcription skill.

Problems of Transcription

Transcription involves hearing the sounds and sound patterns of a language, understanding their meanings, and representing the sounds in the written symbols of the language, inferring unheard or inaudible sounds and words. Understanding the meaning of sets or combinations of sounds is absolutely necessary, especially for those languages such as English, French, or Chinese, for which the graphemic representation (the writing system) generally does not correspond to the phonemic structure (the sound system) of the language. For example, the underlined spellings in the words *shot, schist, session, efficiency, cautious* all represent the same sound (all of which can be represented by the IPA symbol [ʃ]). Cases such as this illustrate that English cannot be transcribed without knowledge of the meaning of the sets of sounds of the language.

Even for those languages whose writing systems are largely phonemic, such as Turkish, Spanish, Japanese, or Korean, understanding of the meaning is indispensable to obtain a correct transcription for several reasons. Firstly, any

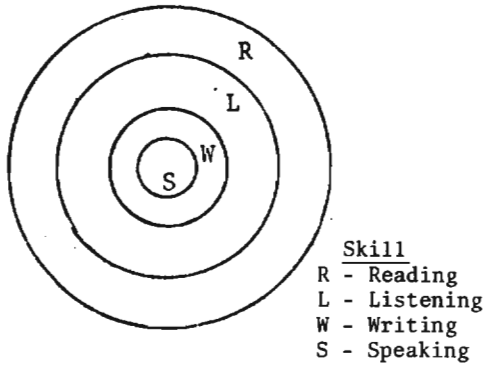
unit of speech sound is articulated differently depending upon its environment. That is, the place and manner of articulation of a consonant will change according to the vowels which accompany it[1]. Secondly, when sounds are articulated in rapid speech or casually, an assimilative tendency[2] to reduce the differences between sounds takes place, and the sounds that a person does utter are the result of a compromise between the assimilative tendency and the minimum differentiation necessary to make himself understood. Thirdly, pronunciation in the spoken form of the language varies, depending upon the social level of the speaker, some group membership, or a personal idiosyncrasy[3]. These allophonic variations are phonetic and do not necessarily signify any change in meaning. However, what seems to be a very small phonetic difference in one's own language may signal a distinct difference in meaning in some other language.

In addition to allophonic difficulties, the listener may not hear clearly everything that is said. This is true even in one's native language. The native speaker, however, can piece together the information from what he does hear because of redundancy[4] in the language and the probabilities of occurrence of certain sequences of sounds. Knowledge of redundancy and probabilities of occurrences of certain linguistic elements built up through experience in the language makes it possible to guess correctly the words that are missing or inaudible. Redundancy in languages is to be found in elements of sound and in morphological and syntactical formations which reinforce each other in the conveying of meaning. The English language, for example, is 50 percent redundant[5]. Without comprehending the meaning, a person cannot take advantage of this redundancy and, consequently, cannot infer missing words.

Relative Skill Ranges

We have found that a significant portion of the transcription skill rests upon the ability to infer missing phonological, morphological, syntactical, and semantic elements as well as to hear the sound patterns of a language and understand and translate the sounds into written symbols. With this in mind we can discuss the relationship of the transcription skill to the other four language skills and analyze the transcription skill range which students should achieve.

When an adult is studying a foreign language, his ideal goal is to achieve the skill range of an educated adult who is native to the language. The relative skill range of an educated native adult may be illustrated as follows:



Relative Skill Ranges of Educated Native Adult

As the diagram suggests, the ranges of reading and listening skills are generally broader than those of writing or speaking. The educated native speaker will be able to recognize and comprehend visually more of the grammatical, lexical, and semantic system of the language than he can recognize and comprehend aurally. Listening requires him to comprehend immediately without deliberation what he has heard. Reading, in contrast, allows for more time to analyze and analogize unfamiliar elements.

Writing requires a more complete and active control of the elements of the language than listening comprehension, and therefore the range of the writing skill of the educated native adult is more limited than the range of listening skill. His writing skill, a productive skill, never surpasses his receptive listening skill ability[6].

The speaking skill, a productive skill, is the most complex skill[7] and therefore is the most limited skill of the educated native adult. Speech requires almost instantaneous interaction between formulations of statements, questions, and replies, while writing is a much slower process which allows more time to deliberate and search for words and forms. Speaking involves thinking of what is to be said while saying what has been thought. Words must be formulated at a rapid rate, with a spacing of about five to ten words ahead of the utterance. In addition, words and patterns must be chosen to fit the right situation or attitude intended.

---

[1]Bertil Malmberg, *Phonetics* (New York: Dover Publications, Inc., 1963), p. 58.

[2]*Ibid.*

[3]Wilga M. Rivers, *Teaching Foreign-Language Skills* (Chicago: The University of Chicago Press, 1968), p. 115.

[4]Claude E. Shannon and Warren Weaver, *The Mathematical Theory of Communication* (Urbana: University of Illinois Press, 1959), p. 104

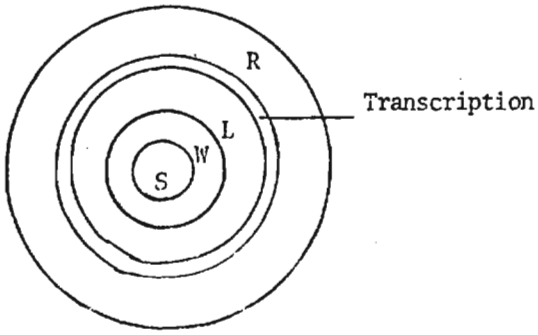
[5]*Ibid.*

[6]Kenneth Chastain, *The Development of Modern Language Skills: Theory to Practice* (Chicago: Rand McNally and Co., 1971), p. 164.

[7]William Francis Mackey, *Language Teaching* (Bloomington: Indiana University Press, 1967), p. 263.

This discussion indicates that the native adult can listen to and understand, and read and understand, more vocabulary and structure than he can speak, and he can demonstrate a greater command of the language in writing than he can in speech. The range of the four language skills of an educated native adult may also correspond to the order of difficulty in acquiring these skills. The speaking skill is the most limited skill of all because it is the most difficult skill to acquire, and the reading skill is the broadest skill of all because it is the easiest one to acquire.

Considering the features and the relationships of the four skills in an educated native speaker, and the features of the transcription skill defined above, the transcription skill may be illustrated in the following diagram in terms of the ranges of skills of an educated native adult and in terms of difficulty of acquisition.



Relative Range of Transcription Skill in Terms of the Four Language Skills of the Native Adult

This diagram suggests that transcription is perhaps easier than listening comprehension. Listening requires retention of information from an ongoing series of sounds and immediate or unconscious comprehension of what has been heard. Transcription does not require that information be retained, nor must comprehension of sounds be immediate and unconscious. In fact, it is sometimes possible to recognize words and write down the words without comprehending their meanings. Transcription is more difficult than reading comprehension, however, because transcription involves recognition of sounds, comprehension of their meanings, and recognition of the words to be copied in the writing system of the languge, and inferring of necessary missing elements. Reading, on the other hand, involves only recognition of written symbols and comprehension of their meaning. We suggest, however, that the listening comprehension skill, which is defined as a receptive skill by most language teachers and scholars, as well as the transcription still, is not a purely receptive skill, but a combination of both receptive and productive skills. The listener always anticipates and predicts certain sequences of sounds with high probabilities of occurrence, and through his knowledge of the language and the factors of redundancy in the language, he actively fills in the sequences of sounds that he does not actually hear or distinguish.

Dependence on the Four Skills

If we assume the transcription skill to be a combination of receptive skill and productive skill, what skills should be developed together with the transcription skill? All language skills are closely related and each language skill complements the other. At the same time, the students' passive knowledge of the components of a language, i.e., phonology, morphology, syntax, and semantics, cannot be deepened, reinforced, and internalized without actively and repeatedly exercising the productive oral skills and the productive written skills. Furthermore, the transcription skill is also a receptive-productive oral skill and, therefore, the speaking skill, which is a productive oral skill, must be developed and used as the means to achieve the development and consolidation of the transcription skill.

Desired Transcription Skill Range

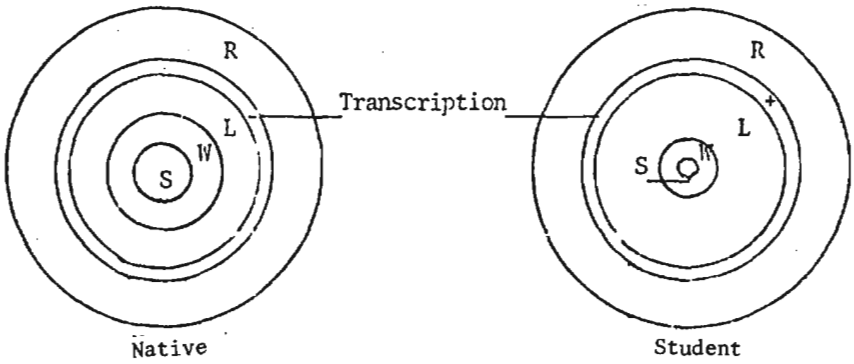
The ideal skill ranges for an adult student to attain in a foreign language are the skill ranges of an educated adult who is native to the language. In the practical situation, however, we recognize that the skill ranges[8] of our students will not correspond to those of a native adult. The students need not acquire as high a level of proficiency in speaking and writing as they do in listening comprehension, transcription, and reading to be able to function satisfactorily in the language. The goal of communication through speaking and writing would be acceptable at a level below that of a native speaker. The minimum skill ranges required in listening comprehension, transcription, and reading, however, are identical to the skill ranges of an educated native adult. The difficulty which the students will experience in acquiring the listening, transcription, and reading skills will therefore be quantitative in nature rather than qualitative. The relative skill abilities of an educated adult who is native to the language and the desired skill ranges of the students are illustrated in the diagram on the next page.

Summary of Concepts

So far, we have discussed the following points:

- Transcription involves hearing the sounds and sound patterns of a language, understanding their meaning, and representing the sounds in the written symbols of the language, while inferring missing linguistic elements;

[8]The concept of different goals for the four different skills originated with Ted Everett.



Relative Skill Ranges of Native Adult
and Desired Skill Ranges of the Student

- The transcription skill is inherently part receptive and part productive;
- The transcription skill should be reinforced by development of the speaking skill, which is a productive oral skill;
- The goal of transcription is to be able to comprehend native speech at normal speed in a real-life nonstereotyped situation. This requires a lengthy period of classroom instruction and on-the-job experience.

Teaching Methods and Techniques

Now that we have discussed the characteristics of the transcription skill, its relationships with the four other language skills, and the desired goal, we will describe methodology and techniques for teaching the transcription skill. In the Korean Department and Japanese Department we have reviewed available information on learning psychology and theories of language teaching, and have adopted the audio-lingual cognitive method (called the "cognitive method" in short) to teach transcription. This method is based upon the assumption that language learning includes a mechanical process and a cognitive process. The idea of the mechanical process of language learning stemmed from the behaviorist theory of stimulus-response learning, particularly as developed in the operant conditioning model of Skinner[9]. This view has been rejected by Chomsky and Lennenberg[10] and other theorists who maintain that there is something more to language learning than the mechanical process of imitation and generalization. They have, instead, emphasized the cognitive aspect of language learning.

We suggest, however, that the process of foreign language learning is built upon both habit formation and the cognitive process and therefore we have incorporated both concepts into five distinct phases of classroom activity. These phases include:

- expository presentation of material;
- analysis of the content through explanation in the native language;
- drills stressing understanding of the content;
- consolidation of those learned patterns through application to new situations; and
- evaluation of the students' level of learning.

The Five Teaching Phases at the 120 Level

- *Presentation*

In this initial stage, students are given written material to study before they listen to recordings. They can study the written text and the accompanying tape before a particular lesson outside of the class if they wish. In the classroom, the teacher first projects the written text on a screen and reads it aloud, alone, as a model. Then the teacher reads it with the students, and/or asks the students to read it in chorus and individually. The objective of this activity is to provide practice in the visual and aural identification of common word groupings, and phonological and structural patterns which are unfamiliar to the students. Memorization of the text, if possible for the student, greatly enhances the students' ability to identify a sequence of sounds and their associated written symbols.

- *Explanation*

After reading the material alound, the teacher and the students analyze grammatical sequences and tenses, modifiers and function words, cliches, expletives, hesitation expressions (which can be ignored as irrelevant to the message), levels of discourse (colloquial or formal), emotional overtones, as well as regional or dialectal variations, and translate them correctly.

Initially, the students at the 120 level usually have little ability in listening and

[9]Rivers, p. 73.
[10]*Ibid.*

speaking and writing, and, therefore, the foreign language utterances strike their ears as a stream of undifferentiated noises. By providing a written text and explaining the meaning thoroughly, we can help the student to assign meaning to these utterances and thereby enable him to transcribe material more efficiently and accurately. The value of this method can be contrasted with the unguided learning situation commonly encountered by immigrants in a foreign land. Lacking explanation of the meaning of sound patterns, immigrants are unable to understand more than a few simple phrases, even after many years of residence. This leads us to assume that aural comprehension must be learned in part through the theoretical framework which is provided by recognition of the meaning of words and phrases.

■ *Manipulation*

After the materials have been visually presented and explained by the teacher, the students listen to and transcribe a recording of the material without benefit of the written text. This drill allows the students to aurally identify a sequence of sounds in meaningful succession and to transcribe them correctly in the writing system of the foreign language, while inferring sounds which they missed or could not identify. Moreover, they utilize the passive knowledge of vocabulary and structure which they have studied and retained from the preceding presentation and explanation activities.

The transcription drill is followed by a drill in which the students read aloud their transcripts in turn and the other students listen to it, correct mistakes, and supply missing sounds and words. At the same time, the teacher helps the students to understand the material by explaining deductively why they made mistakes and what particular phonological, morphological, and syntactical elements are involved.

After the transcriptions are corrected in class, the students listen to the tape recording again and compare their transcript against the sounds on the tape. This exercise reinforces the students' ability to associate sounds, meanings, and written symbols. The students' transcripts are submitted to the teacher after this drill, and the teacher corrects any remaining mistakes. The transcript sheets are returned to the student at the earliest opportunity, on the same day if possible, so that the students will be aware of any mistakes which they missed while correcting their transcripts.

After reviewing the transcript sheets, the class moves on to another drill or drills, such as true-false drills, question-and-answer drills, or reproduction drills. For example, the students are asked to respond "true" or "false" in English to statements which the teacher prepared based upon the text, or the teacher may ask each student to compose a statement and have another student respond "true" or "false." In the question-and-answer drill, the teacher may put questions to the students, the students to the teacher, and/or the students to each other. These drills facilitate the students' ability to recognize word groupings and patterns and to produce them with ease in a sequence and environment which are are slightly different from those in the text.

The various oral drills are indispensable for developing and reinforcing the productive aspect of the transcription skill. Their effectiveness can be easily demonstrated by giving transcription tests. Students with a superior speaking skill and inferior reading skill will perform better than students with an inferior speaking skill and a superior reading skill.

■ *Consolidation*

After the manipulation activities, the students are ready and eager to try their ability at recognizing, understanding, and transcribing vocabulary and structure which they have studied in a totally different context without the use of the prepared written text. The teacher dictates selected material which includes some of the vocabulary and structures which the students have studied. As a challenge, the teacher also includes some unfamiliar vocabulary and structures. The students listen to and transcribe it, and do so with a great sense of achievement when they find that they understand the meaning of what they are transcribing.

A question-and-answer drill follows the dictation drill. This time, the questions and answers are exchanged only among the students. Both form and content are dealt with in the questions and answers. The students at first ask questions about form in order to supply missing words or to correct mistakes. The students then proceed to ask questions concerning the meaning of vocabulary items and then move on to the content of the entire selection. After the question-and-answer drill, each student may be asked to narrate it in his own words.

The teacher's role is kept to a minimum in this activity. He plays the role of consultant, guide, and assistant to the students -- and only when needed. Afterwards, the teacher collects the students' transcription sheets, corrects mistakes, and returns them at the next session in order to advise students of unnoticed or uncorrected mistakes. The teacher may also show the correct transcript on the screen and ask the students to read and translate it for reinforcement.

■ *Evaluation*

After the material has been presented, explained, manipulated, and consolidated, the teacher gives the students a very brief achievement test which covers only what has been taught so far in the course. The test consists of dictation which the teacher presents to the students for transcription, either through the medium of recorded tape or by reading it to

them. The teacher collects the transcription sheets for evaluation and then projects the correct version of the transcription on a scrren. The students are asked to translate this version, and their translations are also collected for evaluation. The transcriptions and translations indicate how much of the material has actually been mastered by the students and serve as the basis for the final grade in the course.

In addition to this type of text, every ten lessons or so the teacher gives a transcription test which does not contain material from the text or which was covered during the consolidation activities, but which is of approximately equal difficulty. The test measures students' growth in the range of their transcription skill since the last such proficiency test. The transcript is corrected by the teacher. It is not used in determining the final grade, however, because the content of the test was not taught to the students.

Course Emphasis

We have discussed the different objectives of the five teaching phases in a 120-level transcription course. The activities of each phase may vary from teacher to teacher or from day to day, but the five teaching and learning phases are distinct and characterize the cognitive method. The five phases are covered each class day, which lasts from 3 to 3½ hours. At the end of the day, the students should be able to transcribe about 200 syllables of dictation with an average of two mistakes. The dictation can be based on material covered in any of the past lessons.

The five phases are emphasized differently for more advanced transcription courses, such as 220 or 320. In general, the higher the course level, the more time is spent on consolidation and evaluation. Emphasis on evaluation activities does not mean that the students are given long tests, but that the students can independently transcribe more material which is unfamiliar in more advanced courses. The 120-level course is fairly tightly controlled by the teacher. The 220 class is an intermediate situation. At the 320 level, the students experience a more unstructured environment which resembles a real-life work situation where totally unfamiliar material must be transcribed every day.

The cognitive method of instruction has so far proven quite successful. Nevertheless, the students are still unable to transcribe all material freely after these courses. The goal of the student is to achieve a transcription skill range which matches that of the native speaker. It must be emphasized that this cannot be successfully achieved without development of the speaking skill, nor can it be achieved without a long period of instruction and on-the-job experience. For example, a recent study of students of Japanese[11] has shown that fluency in the language requires 5 or more years of formal study, including approximately 2 years of residence and study in Japan. The study shows that even after this lengthy period of training, students are still unable to write with ease. An adequate transcription skill range is not easy to achieve, but through the cognitive method and with instruction in the listening comprehension and speaking skills, it is possible to give students the basic tools with which they can achieve the desired transcription skill range.

---

[11]American Council of Learned Societies and the Social Science Research Council, *Japanese Language Studies in the United States: A Report of the Subcommittee on Japanese Language Training Study of the Joint Committee on Japanese Studies* (December 1976), p. 30.

TET, FRED HAND OVER BLUE PENCILS, BRASS KNUCKS

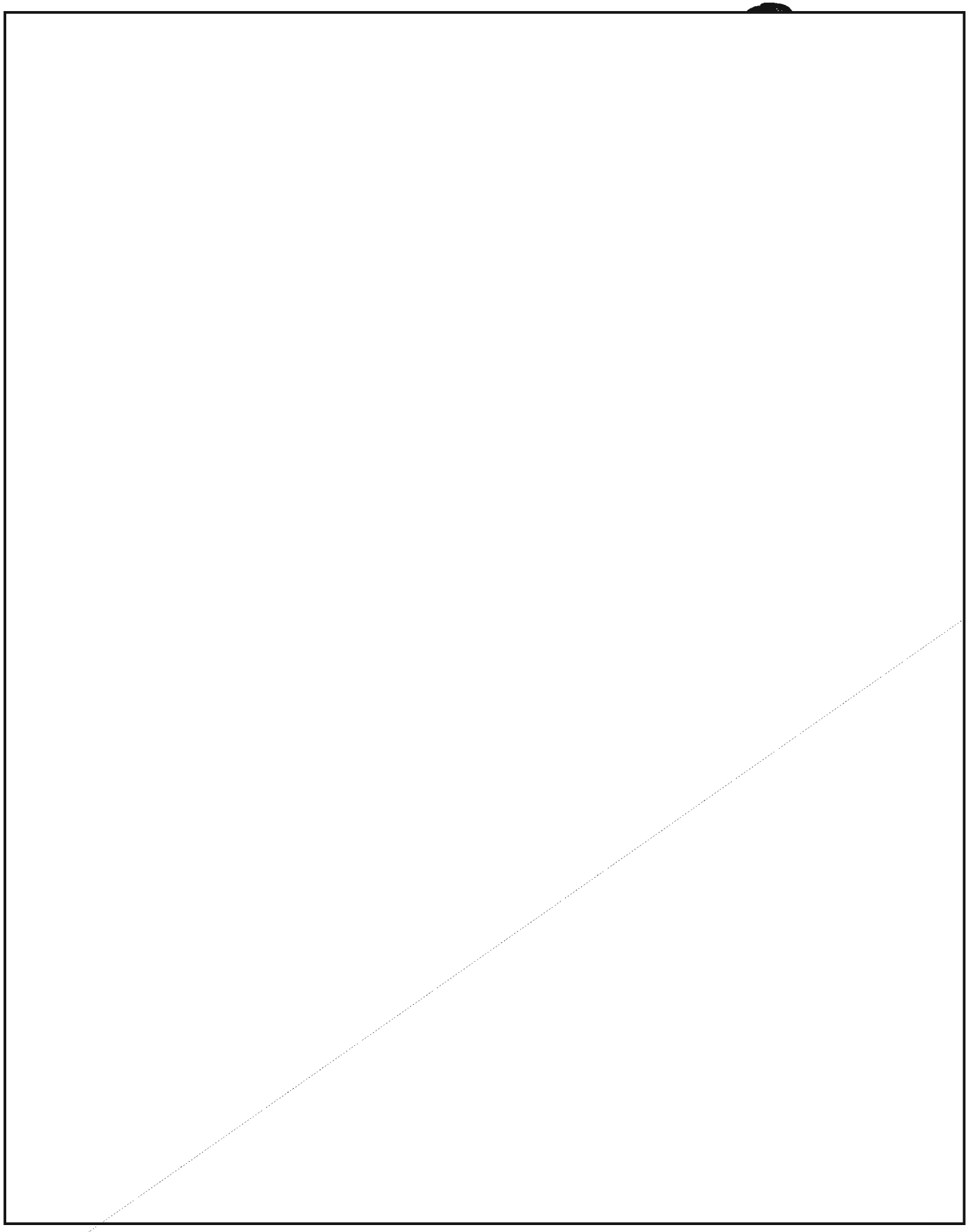
Starting with this issue, there are two changes in the makeup of the Editorial Board: Emery Tetrault (Language Editor since February 1975) and Frederic O. Mason, Jr. (TA Editor since January 1975) have completed tours in which each has made a large contribution to broadening the magazine's readership. In addition to acting as advisor on incoming manuscripts in their respective fields, as well as encouraging and assisting their coworkers to submit articles to CRYPTOLOG, Tet and Fred contributed several articles of their own. Tet wrote "Even a 5-year-Old Child..." (October 1974); cogent letters to the editor (February 1975, April 1977); "Where Does 'Does' Come From?" (June 1975); and "Research in Speech Perception" (August 1976). Fred wrote "TA, Handmaiden of CA" (May 1975); "More on Squaring the Page (A Crypto-TA Function)" (June 1975): "Abdul and His 40 Tanks" (August 1975); "A Vexing Agency-Wide Problem" (November 1976): and "Where Were We?" (January-February 1977).

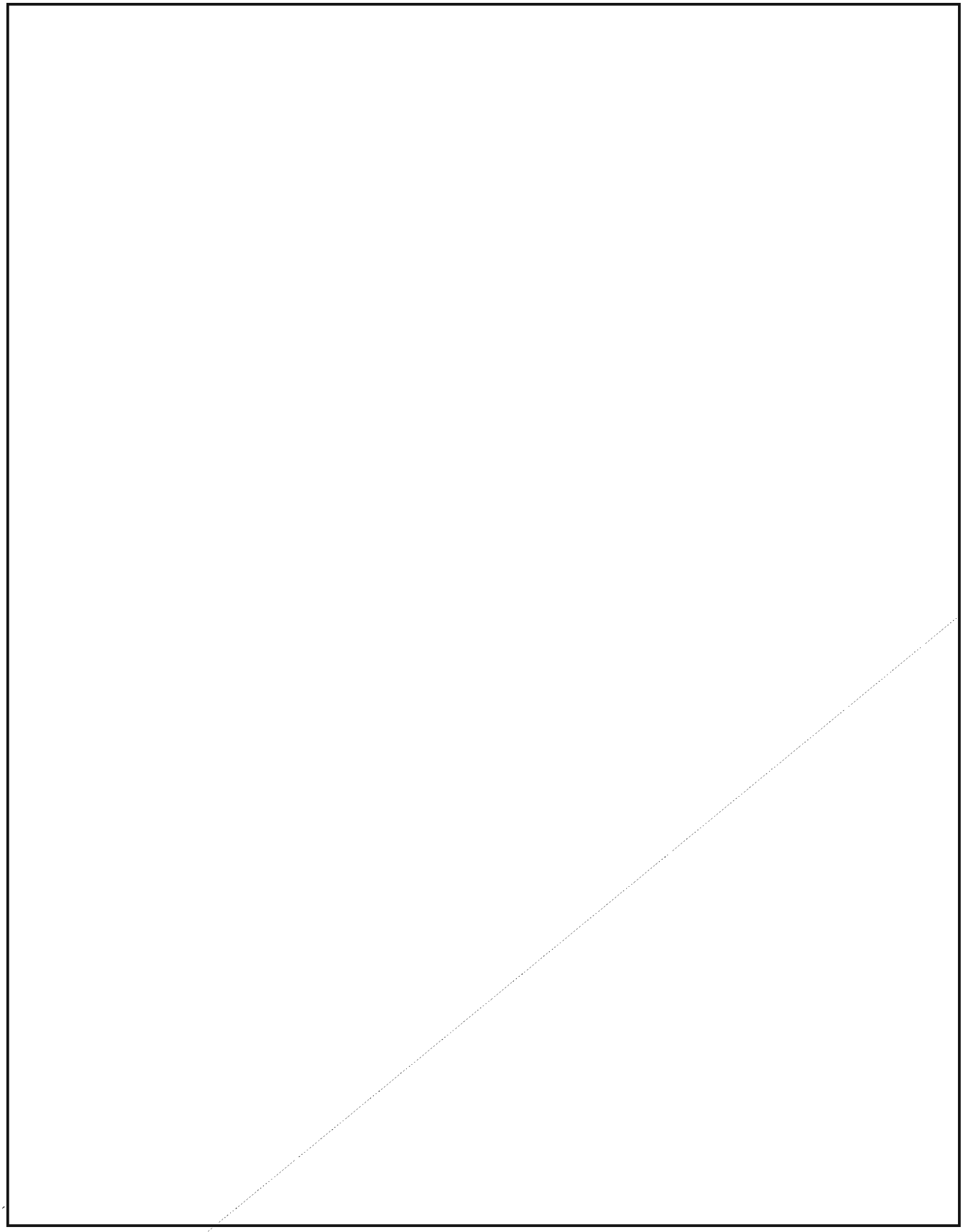
I've appreciated working with Tet and Fred and know that they will continue to share their ideas with CRYPTOLOG readers. Who knows? Maybe now, with no need to persuade others to write articles, they might find lots of time to write many more of their own.

Tet and Fred are being replaced, respectively, by [redacted] have been told that they do not actually have to write articles themselves (although they may, if they want to). But their main job will be to lean on their coworkers and have *them* write about things they know about. So if you linguists and traffic analysts out there hear an increase in occurrences of the exclamation, "Hey, that would make a good article for CRYPTOLOG!", you'll know why.

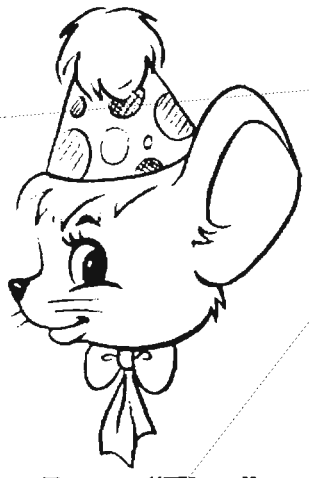
P.L. 86-36

Ed. (UNCLASSIFIED)





Less than **$5,000 in prizes**
Awarded Monthly



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

Draw "Tiny"

YES, WE AWARD LESS THAN $5,000 IN PRIZES MONTHLY TO NEW CRYPTOLOG SUBSCRIBERS!!!

Considerably less than $5,000! In fact, we don't award *any* cash prizes monthly! Or *ever*! But you can still win a subscription to CRYPTOLOG.

Draw "Tiny" any size except like a tracing. Use pencil. (Or simply print your name on the coupon below.) Every entrant receives a free unprofessional estimate of his (or her) drawing (or ability to hand-print).

ALL ENTRANTS ARE WINNERS! Winners will receive a subscription to CRYPTOLOG, one of America's leading TSC in-house publications. Our objective is to find prospective readers who appear to be properly motivated and have an appreciation and liking for this sort of publication.

Your entry will be judged in the month received. Prizes will not be awarded for best drawings of various subjects (or best hand-printing specimens) received from any entrants age 14 (or any age). No drawings (or hand-printing specimens) can be returned. Contest winners will not be notified. Send your entry today.

MAIL THIS COUPON TO ENTER CONTEST

To: CRYPTOLOG,
P1

Please enter my drawing in your monthly contest. (PLEASE PRINT)

Name_____
Organization
~~Occupation~~_____ Age_____
Address N/A Apt. N/A
City N/A State N/A
County N/A Zip N/A
Telephone Number N/A

~~(C)~~

(U)

ZBB? WHAT IN THE WORLD IS THAT?

C263

Early in 1973, at an office meeting, the speaker read the acronym SADPPO, then asked, "What in the world is *that*?" Having just read NSA Regulation 110-2 the day before, I immediately jumped up and unraveled the deep mystery: "Senior ADP Policy Officer!" From that simple statement I was immediately proclaimed the world's foremost authority on SADPPO.

In a way, the same thing happened again recently with the abbreviation ZBB. When I saw it cross my desk for the first time, I was able to jump up mentally and say, "Zero-base budgeting!" Because just a few days earlier, I had read the book by that name (*Zero-Base Budgeting*, by Peter A. Phyrr). Having become, *ipso facto*, the Agency's "ZBB expert," I now feel ready to write an article about it and really establish my field of authorityship.

I'll leave the more intricate details of ZBB to the budget boys, but try to give a glossary-level understanding of the key objectives so that the operational force can find the transition to the new concept easier to take.

I'll purposely avoid using words and phrases such as "decision packages," "ranking, "macro-planning," and "microplanning." It is so easy to become entangled in catch words and phrases, until they become a part of our normal vocabulary even though we are still unable to grasp the main intent of ZBB.

First, ZBB is not just another burden laid on us all, although I have been just told that it is. On the contrary, it is a concept which, if the understanding of it were to filter down to the working level, would ensure that the government gets more for its money. Just as Value Engineering attacks the very premise of our design as possibly not being the best, and Base-Line Management shows us where we are and where we are going (even though we already profess to know), ZBB has as its roots the assumption that there is always an alternative way to solve a problem (even though we doubt it). Dare we admit that there is even the remotest possibility of an alternative to our already perfect plan?

Unlike PERT (Program Evaluation and Review Technique) and CPM (Critical Path Management), which will never concede a need for a slipped date, but only a readjustment of activities or events with slack or float time or alterations to the critical path, ZBB demands that we *do* concede an alternative to our already perfect plan. Years ago, in a Work Simplification course, the professor gave our class a project to cut the time, and thereby the cost, of a simple manufacturing process that had already been "simplified" by three previous classes. It was utterly impossible for us to cut the time any more. Or so it seemed to us, until the professor very humbly suggested an alternative: instead of shortening the process, we could eliminate it completely. We were all very quiet until the next class.

IN ZBB, not only must we concede that there must be alternatives to our plan, but we must further concede that they are cost-related. If we can swallow that much crow, we are ready for Step 2: that someone else will undoubtedly evaluate our alternatives and then, possibly, have the audacity to place our second choice first.

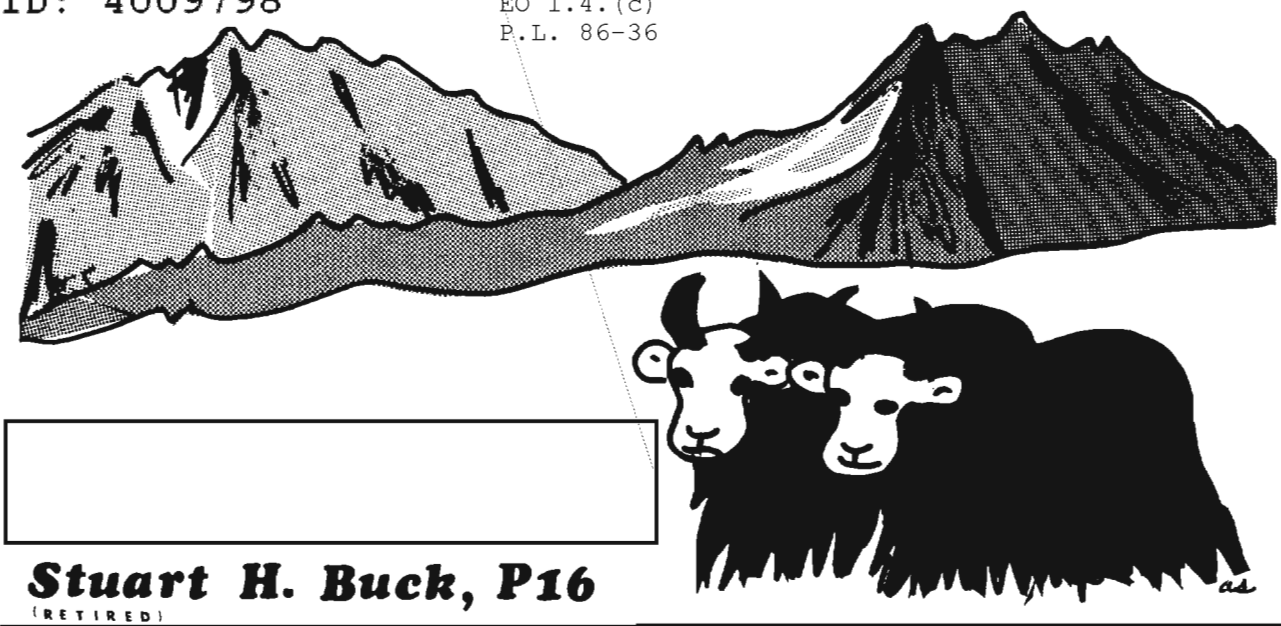
For it is on this tenet that ZBB draws its strength: that there *are* alternatives and that these alternatives must be ranked as to their cost-effectiveness value within the relationship of the total budget which was reached mainly through the workings of PPB (Planning Programming Budgeting). Also, ZBB requires that we point out in each alternative the consequences of not doing something. As programs progress, so do the alternatives. Therefore, industry has found ZBB most useful for budgeting non-production expenses, because of its flexibility.

"What about PPB?" someone may ask. Does ZBB negate PPB, or does it supersede it? Neither! The two concepts work together. We still require top-level, long-range planning. The big difference now involves the low-level, short-range planning, with cost-related alternatives. Except that, with ZBB, we are soliciting our budgeting aid from the grass-roots level.

Does ZBB affect us in our negotiations with the contractor? Absolutely yes, particularly where an RFQ (Request for Quote) is sought. It's back to the crow-eating example. Are we willing to ask our contractor to use his expertise and initiative to devise an alternative to our already perfect task description in the project directive? Remember, he is an expert and the best qualified, or we would not have picked him.

What if we're planning a really big project and we know it's going to cost more than what is available? What do we do? Cry a little and lie a lot? Or plan only enough to get started? It's "none of the above." Instead, we consider the alternatives. And then we look for *more* alternatives.

(Continued on page 20)

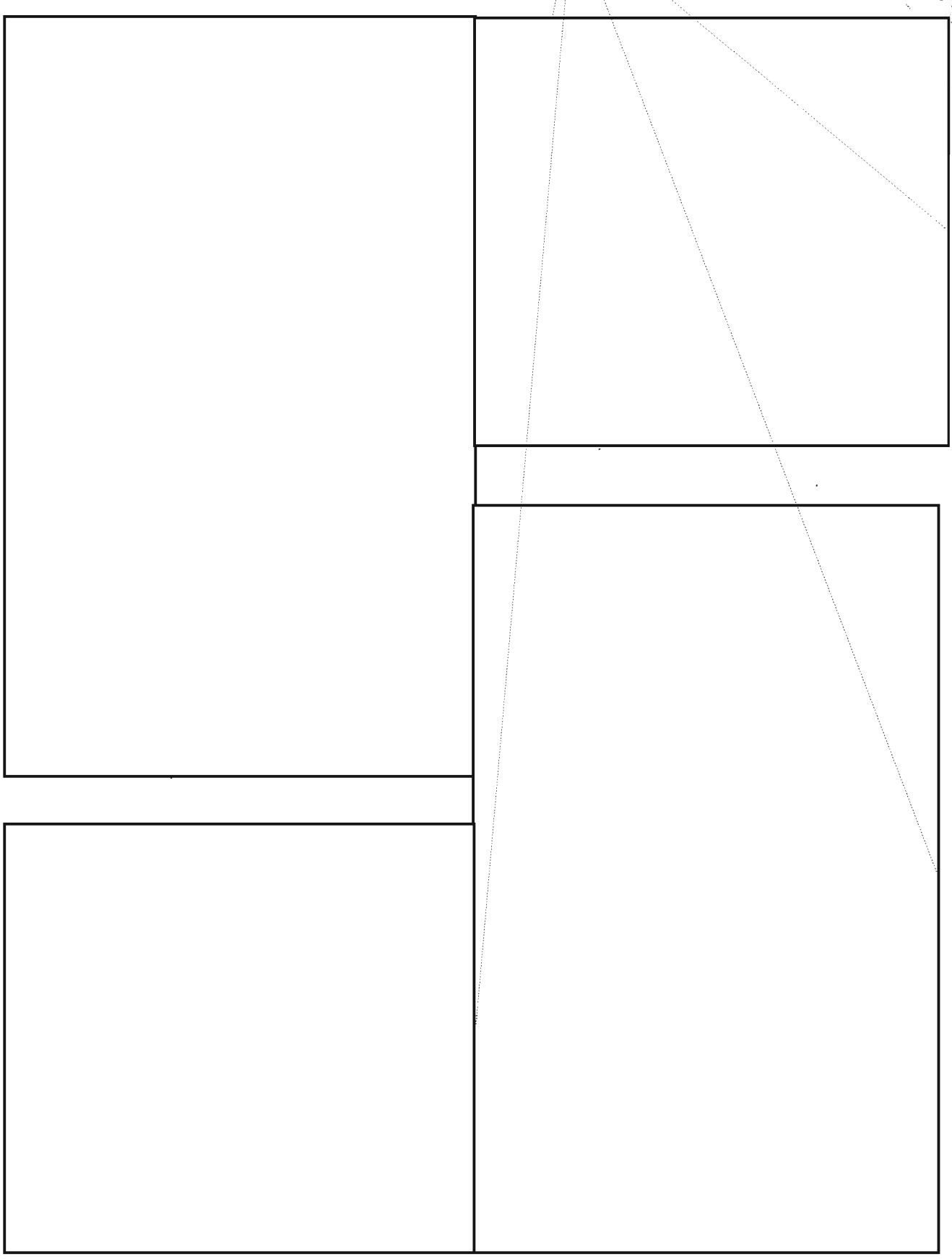


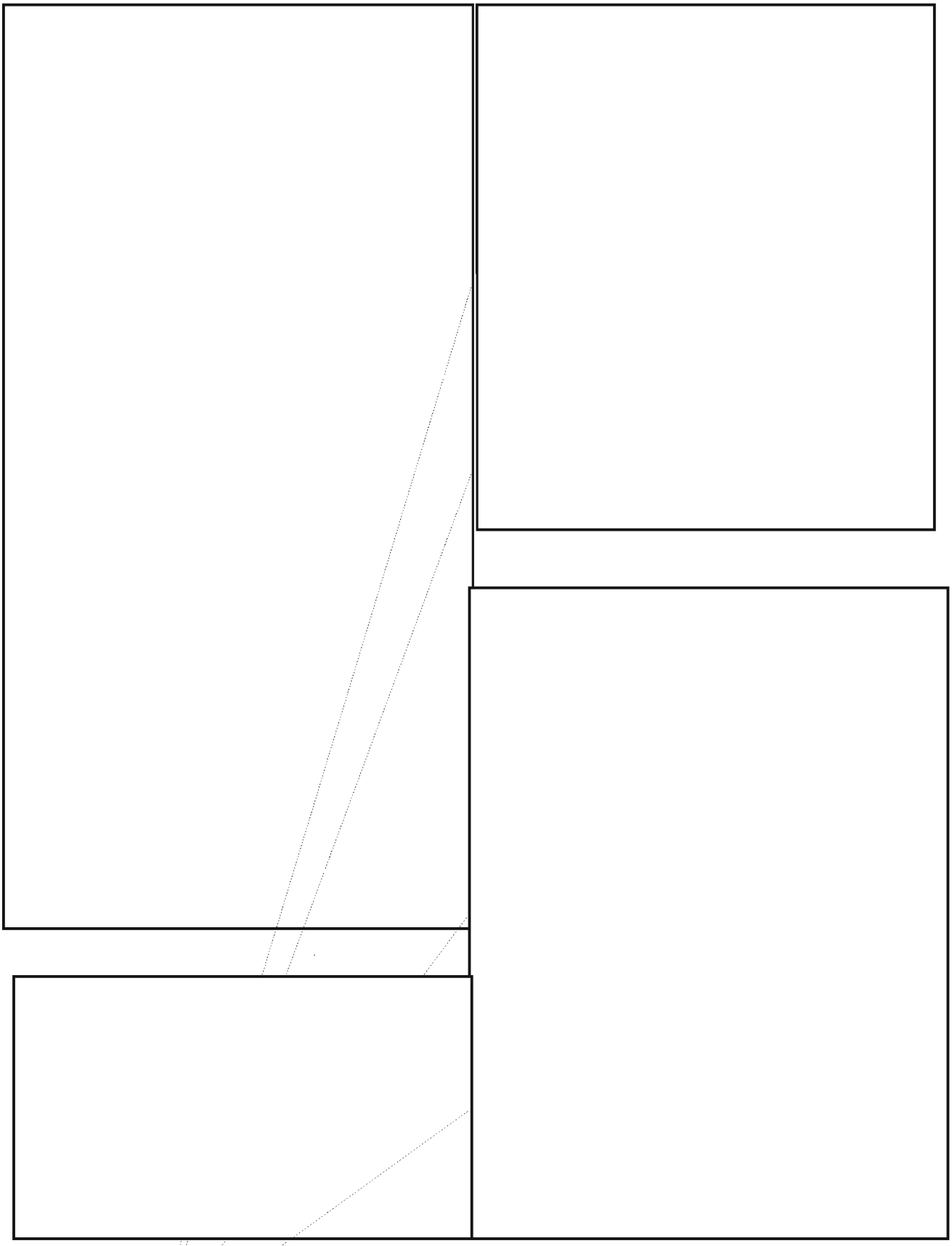
Stuart H. Buck, P16
(RETIRED)

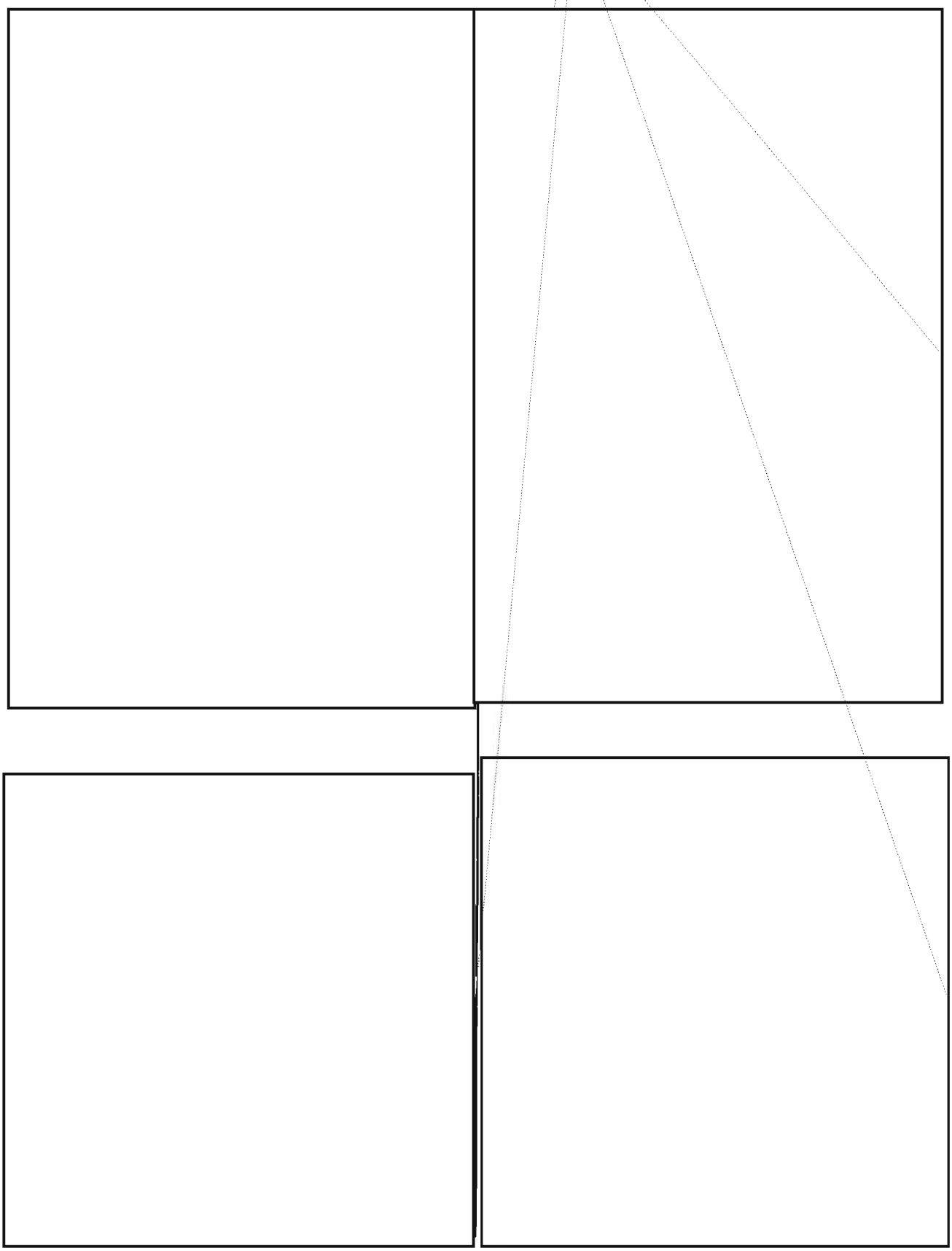
Before dwelling further on this thought, I think it would be advisable to define what we mean by bookbreaking, as used in the context of this talk. This is a ticklish subject, guaranteed to inflame tempers. Bookbreakers, as a group, are much like the blind men and the elephant -- they seem incapable of distinguishing the whole beast from the one small portion that they happen to touch. A common assumption is, "All codes are like the one that I once worked on. . ." Nothing could be farther from the truth. In fact, it is impossible to have a meaningful discussion of bookbreaking without clearing up certain common misconceptions.

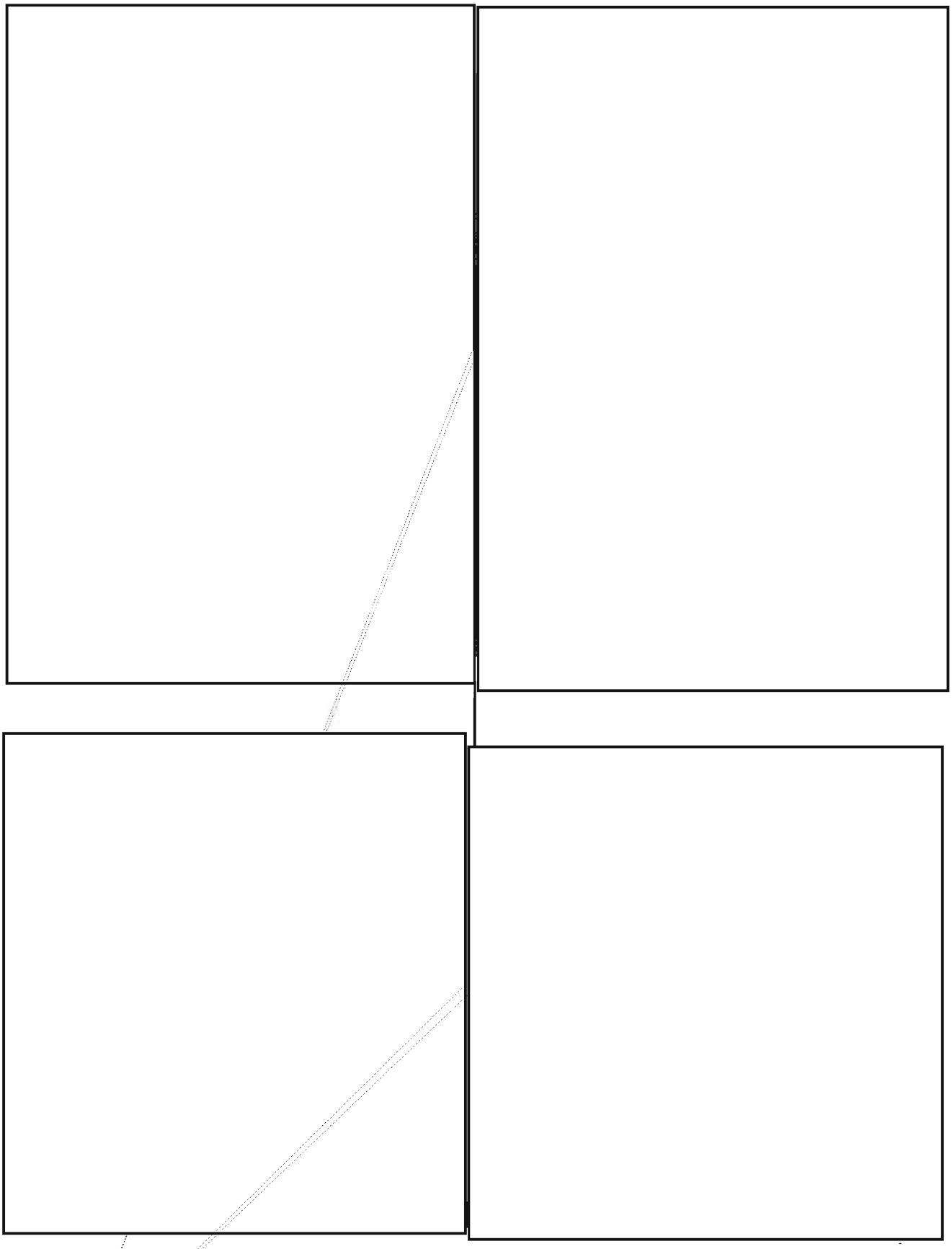
First, we had better settle the whole business of code charts as opposed to code books, the area where most of the misunderstanding begins. It is absolutely vital to understand the difference between these two broad categories; otherwise, our present thesis will make little sense. Generally speaking, code charts are made up of blocks of information or specific categories

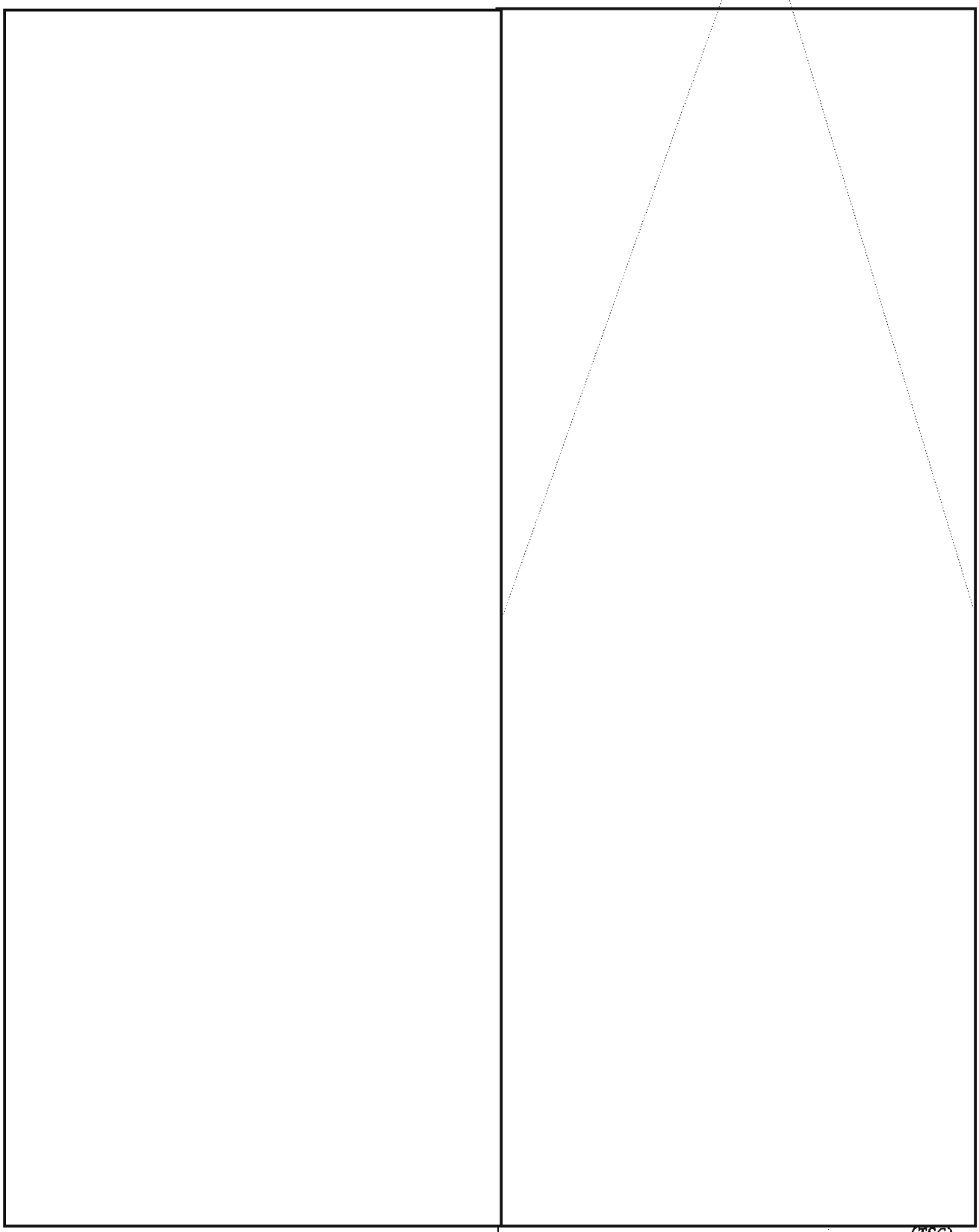
that have a definite beginning and ending, each with a built-in logic of its own. In other words, they are *finite*. Common examples are: numbers, the alphabet, a syllabary, years, months, days, time of day, etc. If the chart is intended for the routine operations of a particular organization (as it usually is), it may contain special category blocks, such as types of aircraft, names of vessels, ports, airfields, points of the compass, weather conditions, and so forth. Actual vocabulary included in such charts is limited to the immediate needs of the users. After all, words not on the chart can be easily spelled out, using either the alphabet or the syllabary, or both. Code charts of this type are a cryptanalyst's delight. All you have to do is to break into a category in a couple of places, then generate the rest. Moreover, each chart is subject-oriented to a high degree. Ships don't fly, aircraft don't drop anchor, and the weather, however disagreeable, can do just so many things. You might have to consult with a linguist occasionally to make sure that things are going right, but, for the most part, the problem-solver happily thinks in English -- and usually gets away with it. In the end, he arrives at a total solution, just as in a crossword puzzle. Decrypted messages are then handed over, not to the person who solved the puzzle (because he can't read them), but to a linguist, who, presumably, functions at a lower level.











~~(TSC)~~

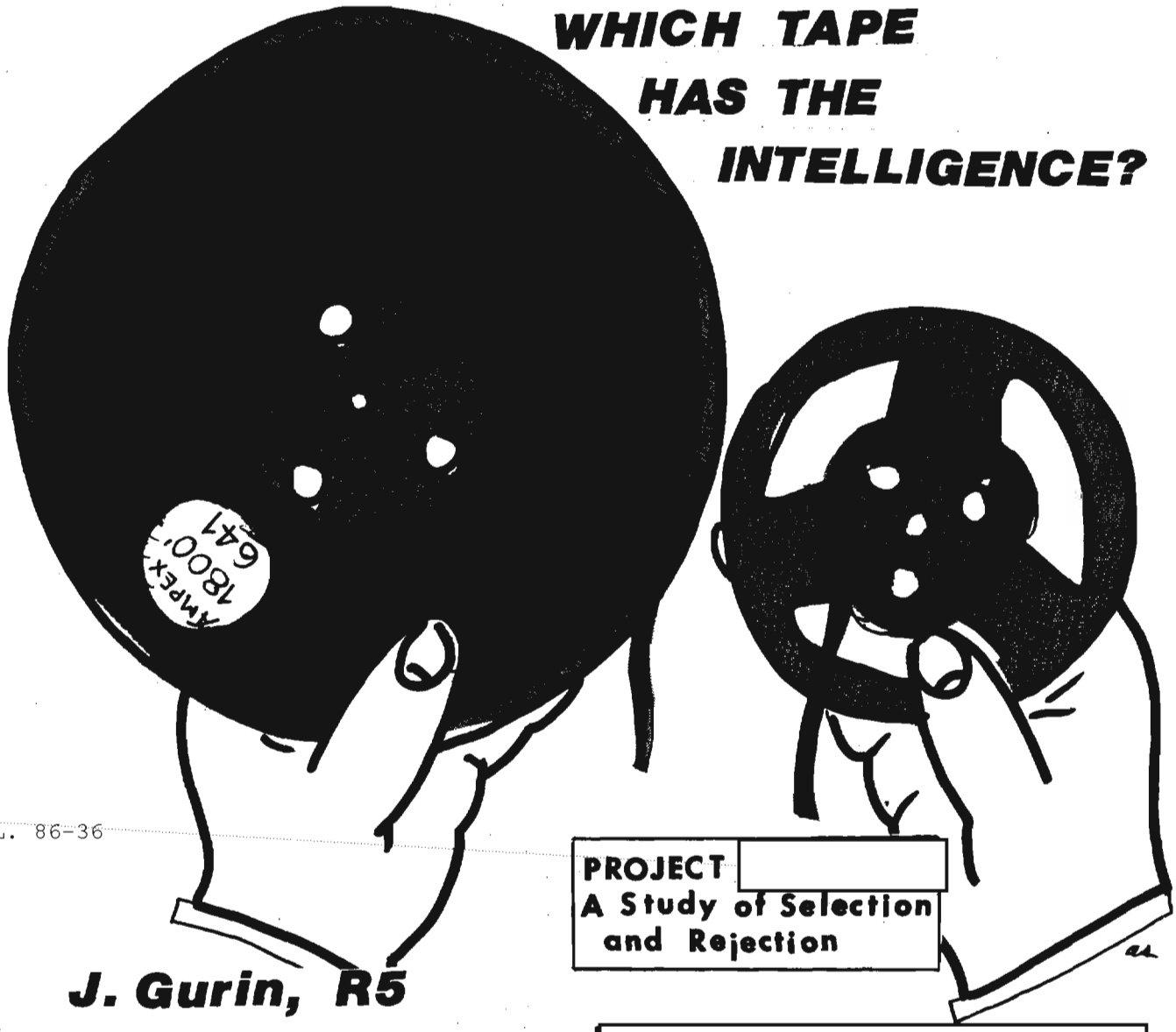
As we saw in the preceding article, Stu Buck accomplished a feat in the tradition of Champollion and Ventris, applying techniques that evolved over centuries of studying ancient texts. Some of the aids Stu referred to were so well described by [redacted] (now retired) that her comments are reproduced below, somewhat abridged for reasons of space. Her unabridged comments are contained in *Bookbreakers Workshop 1970*, the proceedings of a series of 14 sessions sponsored by P1 and chaired by Stu. Copies of the publication (TSC, S-212,800) can be obtained from Harry Goff, P16, 4998 S.

[redacted]
Chairman, Bookbreakers Forum

[redacted]

[redacted]

WHICH TAPE HAS THE INTELLIGENCE?



P.L. 86-36

PROJECT [redacted] A Study of Selection and Rejection

J. Gurin, R5

A certain excitement seems to have been generated by a modest project, devised in the Office of Research (R5) and under way in A6. It purports to discover how decisions are made either to retain or to reject intercepted conversations. No doubt the excitement is related to the desire, or even anxiety, of those who are seeking some way in which the machine may help solve the problem of too much traffic for too few transcribers. Project [redacted] under way for several months, is attempting to pin down the precise factors which enter into the human decision-making act, in the hope that much will be learned that will be of value in the eventual automation of some part of the process.

[redacted]

[redacted]

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

It may seem odd that we have never examined our selection mechanism in this way until now, but perhaps the need was never felt so acutely. Whether we succeed eventually in automating some significant portion of the process or not, we should gain some useful insight into the process and benefit in some other ways as a result of this investigation.

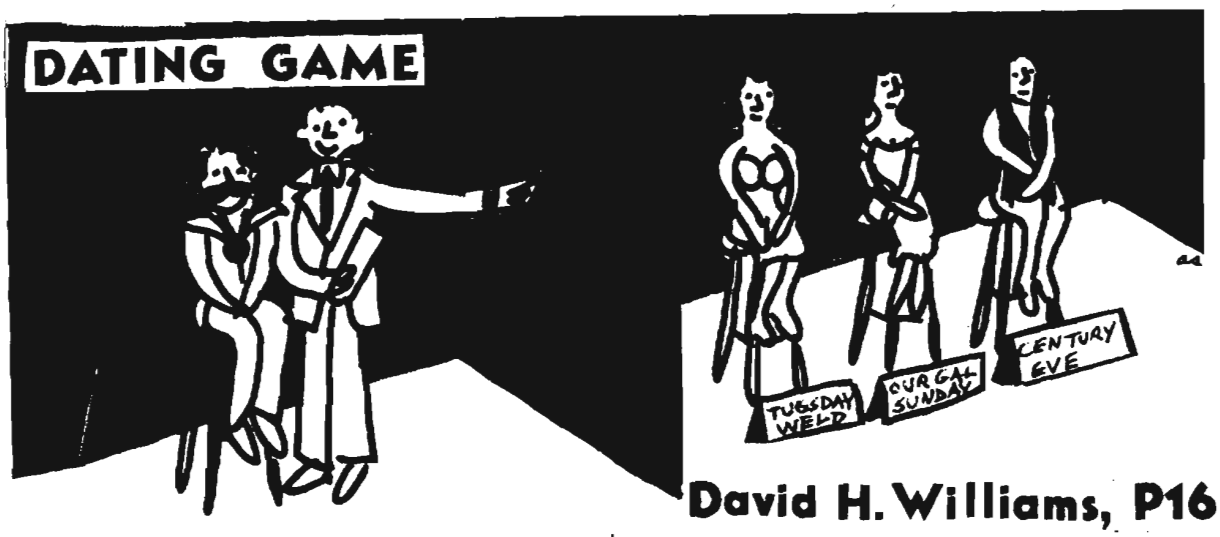
~~(CONFIDENTIAL — CCO)~~

(Continued from page 10)

To imply that this is all there is to ZBB and that it is as simple as this brief introduction might indicate is to discredit ZBB grossly. So don't stop here! Read up on it! There is plenty of good material available at the C5 Library, including the following:

- *Zero-Base Budgeting*, Peter A. Phyrr (HF5550. P99);
- *Zero-Base Budgeting Comes of Age*, Logan Cheek, American Management Association;
- "Annual Overhaul," Lindley H. Clark, Jr., *Wall Street Journal*, 14 March 1977, p. 1;
- White House Memo, dated February 14, 1977, signed by President Jimmy Carter, with attachment by Burt Lance, Director DMB; with working draft of instructions for agencies in designing and implementing their internal zero-base budgeting systems;
- *Planning Programming Budgeting*, Fremont J. Lyden (HJ2052. L98);
- *The Politics and Economics of Public Spending*, Charles L. Schultze (HJ2052. Sch8).

(UNCLASSIFIED)



David H. Williams, P16

Have you ever found yourself needing to know the day of the week that some date fell on several years ago, and been unable to find a calendar for the proper year? If so, you might be interested in the following method for determining the day of the week by a bit of arithmetic simple enough to do in your head. The system looks more complicated than it actually is. In the course of preparing this article, I taught the system, as an experiment, to a 13-year old. It took 15 minutes.

The formula is quite simple:

$$Y + L + M + D = N,$$

where Y is the last two digits of the year,

L (leap year factor) is $\frac{Y}{4}$ (ignoring any remainder;

M is the month additive;

D is the date; and

N is the day-of-the-week factor.

The month additives are:

JaFeMr	ApMyJn	JlAuSe	OcNoDe
1 4 4	0 2 5	0 3 6	1 4 6

These must be memorized. It helps if you think of the first three triplets as perfect squares.

To determine day of the week, divide the day-of-the-week factor (sum N) by 7, and, ignoring the quotient, convert the *remainder* thus:

1	2	3	4	5	6	0
Su	Mo	Tu	We	Th	Fr	Sa

Examples:

1. What day of the week did December 7, 1941 fall on?

$$Y + L + M + D = N$$
$$41 + 10 + 6 + 7 = 64$$

Answer: $\frac{64}{7}$ yields a remainder of 1, equating to *Sunday*.

2. What day of the week will December 31, 1999 fall on?

$$Y + L + M + D = N$$
$$99 + 24 + 6 + 31 = 160$$

Answer: $\frac{160}{7}$ yields a remainder of 6, equating to *Friday*.

Obviously, with dates late in the month or late in the century, or both, the arithmetic gets a little cumbersome. Since you're shooting for the remainder after dividing by 7, you can simplify the process by eliminating 7s as you go along. That is, if Y or L or D is greater than 7, simply divide it by 7, and use the remainder in the formula. Likewise when your running subtotal (ST) exceeds 7, reduce it similarly. Thus, the Pearl Harbor example becomes:

$$\begin{array}{ccccccc} Y & L & ST & M & ST & D & N \\ 6 & + 3 = & 9 \rightarrow 2 & + 6 = & 8 \rightarrow 1 & + 0 = & 1 \text{ (Sunday)} \end{array}$$

And the bulky arithmetic of the Century Eve* example simplifies to:

$$\begin{array}{ccccccc} Y & L & M & ST & D & N & \\ 1 & + 3 + & 6 = & 10 \rightarrow 3 & + 3 = & 6 & \text{(Friday)} \end{array}$$

Since I've found that about half my usages of this method involve dates in the current year, I always keep the current Y + L subtotal in mind. For 1977 it's 5. Thus, determining, say, what day Christmas falls on is an easy 5 + 6 + 4 = 1 (Sunday).

For January and February of leap years, subtract 1 from N.

For dates in the twenty-first century, subtract 1 from N; for those in the nineteenth century, add 2.

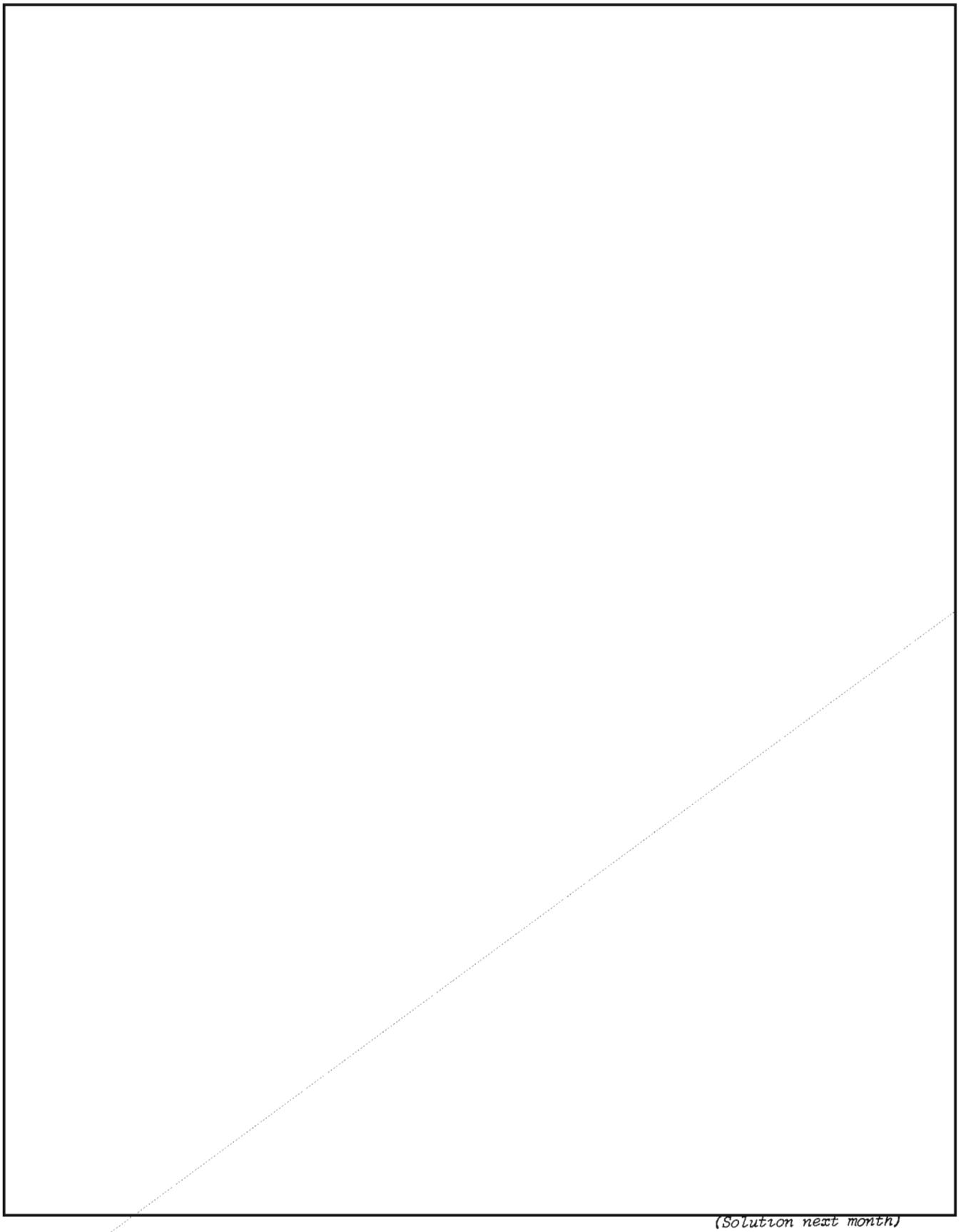
**Editor's note:* I certainly hope that Dave and I are alive on December 31, 1999 so that I can see the incredulous look on his face when I tell him that that date is *not* Century Eve (or even Millenium Eve) and he's a year early with his funny hat and noisemaker.

NSA-crostic No. 8

By A.J.S.

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

DEFINITIONS *WORDS*



(Solution next month)

~~CONFIDENTIAL~~

CORNER

[redacted] P.L. 86-36

DDO Classification Advisory Officer

With this issue, CRYPTOLOG is starting a series devoted to improving classification procedures. From time to time we shall print brief articles that are designed to help the reader in maintaining good classification practices while carrying out his or her everyday duties. Readers are invited to send in questions on difficult classification problems that they would like [redacted] to discuss in future issues, or to send in their own brief articles dealing with classification matters to "Classification Corner."

Ed.

Are there standardized abbreviations for classifications, or can people make up their own abbreviations? Nowadays it's a common thing to pick up papers -- messages, memos, correspondence, etc. -- with various classification abbreviations being used to designate individual paragraphs or titles. The information in one report may be SECRET COMINT Category II, and yet one originator uses the abbreviation "(SCW)" as the abbreviation, another uses "(SS)", and a third uses "(SC)". Do all three abbreviations mean the same thing? Can we use any of them interchangeably? Or is only one correct? If so, which one?

What would you do if you had to take the three reports with the different abbreviations and consolidate them into a single memorandum to be sent forward? Could you look somewhere for the correct abbreviation? The answer is, "Yes, in the *NSA Classification Manual*." That manual lists, on page 28a, all the classification abbreviations as standardized for use in NSA/CSS correspondence. They are the following:

[redacted] P.L. 86-36

First letter(s) indicating the National Classification Level:

TS - TOP SECRET
S - SECRET
C - CONFIDENTIAL
U - UNCLASSIFIED

Second letter(s) indicating special handling:

C - COMINT Codeword
CCO - Handle via COMINT Channels Only

These abbreviations are always enclosed by parentheses, e. g., (TS), (U).

When using the letter "C," do not use a hyphen, slash, space, or other separator, e. g., (TSC), (SC).

But *do* use a hyphen with the abbreviation "CCO", e. g., (TS-CCO), (S-CCO).

With all other special-handling caveats, phrases, or instructions, use a space to separate it from the first letter(s). For example:

(S-CCO NOFORN)	(SC FRONTO)
(TS NOFORN)	(TSC ISHTAR)
(S FRONTO)	(TSC GAMMA)

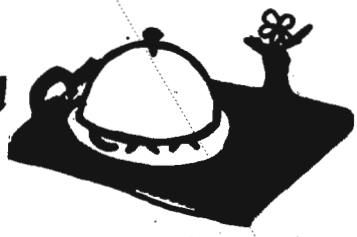
The only instance when a slash is used instead of a space is when using a codeword that is not normally associated with the National Level classification:

(TS/SPOKE)

~~(C-CCO)~~

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

What Ever Happened to the CAA?



[redacted]

P14

Funny you should ask! In January 1977 a new Board of Directors for CAA was elected:

President: [redacted]
President-Elect: David Gaddy
Treasurer: Timothy Murphy
Secretary:
Board Members: [redacted]

Since then, we have been asking around, "What do you think the CAA should be doing?" Some people answered, "Never heard of the CAA!" Others asked, "What ever happened to the CAA?" Still others said, "I thought the CAA died when I stopped seeing COMMAND." And on and on.

Well, let's begin with basics. What *is* the CAA and what is it *supposed* to be doing? The NSA Communications Analysis Assocation has as its purpose, according to its charter:

What - to promote professional growth and outstanding accomplishments;

Where - throughout the U.S. cryptologic community;

How - stimulate new ideas in the analysis of cryptologic problems;
- promote professional contacts and exchange of ideas between analysts in related career fields;
- encourage writing and publication of significant contributions to communications analysis;
- establish a forum for workshops, special interest groups, lectures, etc.

Who - members of the several fields of communications analysis:

- Traffic Analysis
- Special Research
- Signals Collection
- Signals Analysis
- Cryptanalysis
- Communications Security

So, what has the Board been doing? We meet at least once a month, and the meetings are open. You are invited to come out and see for yourself what is going on. Come and tell us where the CAA should be going and what it should be doing.

- We have been lining up speakers for general sessions in the Auditorium: Dave Gaddy in May, Cecil Phillips in June. (Did you miss them?) Watch for the announcements on who our speakers will be. Better yet, join CAA and let us send you your very own copy of the announcements, so that you won't miss any speakers. Other possible speakers at press time (mid-May) include Dr. Telford Taylor, an expert on World War II cryptology and now a professor at Columbia; [redacted]

- A small Special Interest Group on Crypto-TA problems has been started under the leadership of Fred Mason. Other SIGs could be developed, wherever there is enough interest. The Board has taken the attitude that CAA should serve all members and a wide variety of interdisciplines, even if some of the subjects don't have the broad general appeal of a presentation in the Auditorium. Therefore, if some things are interesting to only a smaller, select audience, we're ready to book a smaller room rather than the Auditorium.

Finally, where does the CAA seem to be headed? That's not so easy to answer. Our crystal ball is a little cloudy. Nevertheless, the Board seems to be moving in the following areas:

- In June (still in the future as of this writing), we will have a social get-together -- a cocktail party for Past President [redacted] (departing for NCPAC). Depending upon the response, we'll have more of this sort of thing.
- We are actively discussing (with DDM and others) just what role the CAA could play in post-certification growth. Since we are an interdisciplinary organization, and most notions about what happens after professionalization lean in the direction of cross-discipline work or study, we are beginning to think the CAA could be useful in this area.
- We will continue to look for opportunities to "light fires by rubbing two skills together." There has always been a need to get analytic people to look beyond their own immediate territories, to see how "what I do" might be connected with "what you do." This need is ever-present, both before and after certification (and some career panels have included in their criteria some form of encouragement for aspirants to "get out and see" how other analytic skills live and work).

We're not proud! We'll accept ideas, suggestions, and criticism from anybody. So, what do you want the CAA to do? Where do you want the CAA to go (figuratively speaking)?

Letters to the Editor

To the Editor, CRYPTOLOG:

I am distressed that the reaction to my article on "Integrated Analysts for Asia: A Cohesive Approach" (CRYPTOLOG, August 1976) has centered on an observation I made regarding the Asian male (not my personal) attitude towards women. "Firebrand" (CRYPTOLOG, October 1976) alleges that I have virtually admitted to sex discrimination in the placement of integrated analysts, and Mr. Newton (CRYPTOLOG, April 1977) states that I discourage "utilizing women as employees," which seems a bit much.

Before I am given the "MCP of the Year" award, or disfigured, or something, let me, once again, state what I was trying to achieve in that article. The point I was trying to make is that I believe we need a cyclical program of development for the very few, highly important, integrated analytic jobs which we support, and such a program may require several years (rather than a few months) of preparation by the selectee before deployment. Further, we should, insofar as possible, try to identify those people who will have the best chance of success with [redacted] counterparts and to do so requires an understanding of the counterpart mores, customs, and attitudes.

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

You might be interested to know that before I submitted my article to CRYPTOLOG I had it reviewed by a senior female employee of the Agency whom I have known and respected for several years. This individual is, herself, very active in insuring equality of rights and opportunity for women in the Agency, [redacted] She found my observations to be neither offensive nor inflammatory in the context of the article since she allowed that, while she personally did not like the Asian male attitude toward woman (and what U.S. woman would?), my portrayal of that attitude was accurate within her experience, and was worth noting. She also felt that any woman considering applying for one of the integrated analytic jobs should be aware of what she would be confronted with, and cognitively be prepared to deal with

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

~~CONFIDENTIAL~~

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

it if she were selected. If would appear, if nothing else, my article has achieved this latter effect; although I would welcome some opinion on the program I proposed beyond the particular point at hand.

[redacted] I must confess that my observations of last summer were somewhat superficial. These people have attitudinal idiosyncracies which I never even started to consider. For example, a left-handed person is considered inferior and parents will expend much time and energy retraining a lefty early in life. Another inferior being is a person who drives his or her own car -- if you can afford the car, you surely can afford a driver! And on it goes.

[redacted]

I hope the above will put to rest any sexist charges still pending against me. My point was not to malign the fine women of our Agency or suggest a process in violation of any Executive Order, Personnel Regulation, etc., [redacted] However, the times are changing...

[redacted]

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

To the Editor, CRYPTOLOG:

At the risk of jumping on the proverbial bandwagon or otherwise blowing a rather innocent article completely out of proportion, I, for one, would like to register a bit of moral support for [redacted] concerning his comments regarding women in Integrated Analyst positions. I know he would like to put the entire matter to rest, but it appears that there are those who either thrive on the art of disagreement or otherwise simply refuse to address facts or face reality, especially a reality over which they have *no control*. That is, after all, the root of this entire discussion.

With no intent of disrespect, either for our President or Director, it is evident that the quoted Executive Order 11478 is a work of naiveté. Our foreign friends (the few that still really like us) more often than not are willing to go along with our American customs and standards for a number of reasons -- usually borne of politeness, economy or fashion. He is extremely naive, however, who thinks that by simply issuing an Executive Order, our friends will buckle under and change native habits and customs [redacted] Some are changing, but it's terribly slow and due to worldwide social development, not the whims and desires of *our* women, *our* President, or *our* Agency. That is fact. That is reality.

[redacted] They are great people and they (the men) love their women deeply, and respect them. In fact, behind the scenes the women are more often than not both the driving and stabilizing force in the man's life. But *in public, at work* it's a man's world. That is fact. That is reality.

Can we follow the Executive Order and select a female for an integrated position? Sure. If she is qualified, why not? Should we select a female? To answer this question and to be reasonable, we must go beyond the Executive Order and the American ideal. If an integrated analyst is going to function and be effective in pursuing the assigned mission, he/she must have the mutual respect and credibility of foreign counterparts. If, however, the counterparts do not wish to share that feeling a female due to their own customs and standards, well, that's *life*, and all the Executive Orders, Lib movements, and the like are not going to change it, at least not in the next few years. If, on the other hand, it can be categorically determined that the moot principle and/or spirit of the Executive Order are more important than lasting foreign friendships and hard-won intelligence relationships so necessary to support our National Mission objectives, then perhaps we should press on with same, regardless of the cost.

That is fact. That is reality, guys and girls. If you (both selectees and selectors) fully understand the rules of the game and still desire to fill a specific Integrated Analyst position, then proceed post haste, albeit not blindly in a bureaucratic fog.

Heaven only knows, 6 months of looking at [redacted] fuzzy beard is about all I can take, and a change of scenery would be most welcome!

[redacted]

~~(CONFIDENTIAL)~~

To the Editor, CRYPTOLOG:

Could you please arrange to send me a copy of your exciting, fast-paced, and informative journal each month?

I have heard that the magazine is free, but if this is not the case, I would be happy to give you a recording of "Georgie, Handle the Cows Well" as sung in the original Romanian by

~~CONFIDENTIAL~~

P.L. 86-36

the Brothers Petreusi, in exchange for a one-year subscription.

Thank you very much.

[redacted]

Editor's reply:

No, thank *you* very much!. . . for those complimentary adjectives. If CRYPTOLOG really is "exciting, fast-paced, and informative," it's because of readers like yourself -- people who are willing to send in their letters and their articles, and thus to share their most valuable possessions -- their ideas, their gripes, their suggestions, their honest accounts of successes achieved and failures experienced. We're always pleased to add new names to our subscription list, but even more pleased when new names appear in the table of contents. So, although we appreciate your offer of that choice recording, we would rather have you send us an article we can print. What have you done lately that you're proud of? Or disappointed in? Or mad about? What would you want to share with other CRYPTOLOG readers? Quick, start writing!

(UNCLASSIFIED)

MATCH THEM UP!

By [redacted] D5

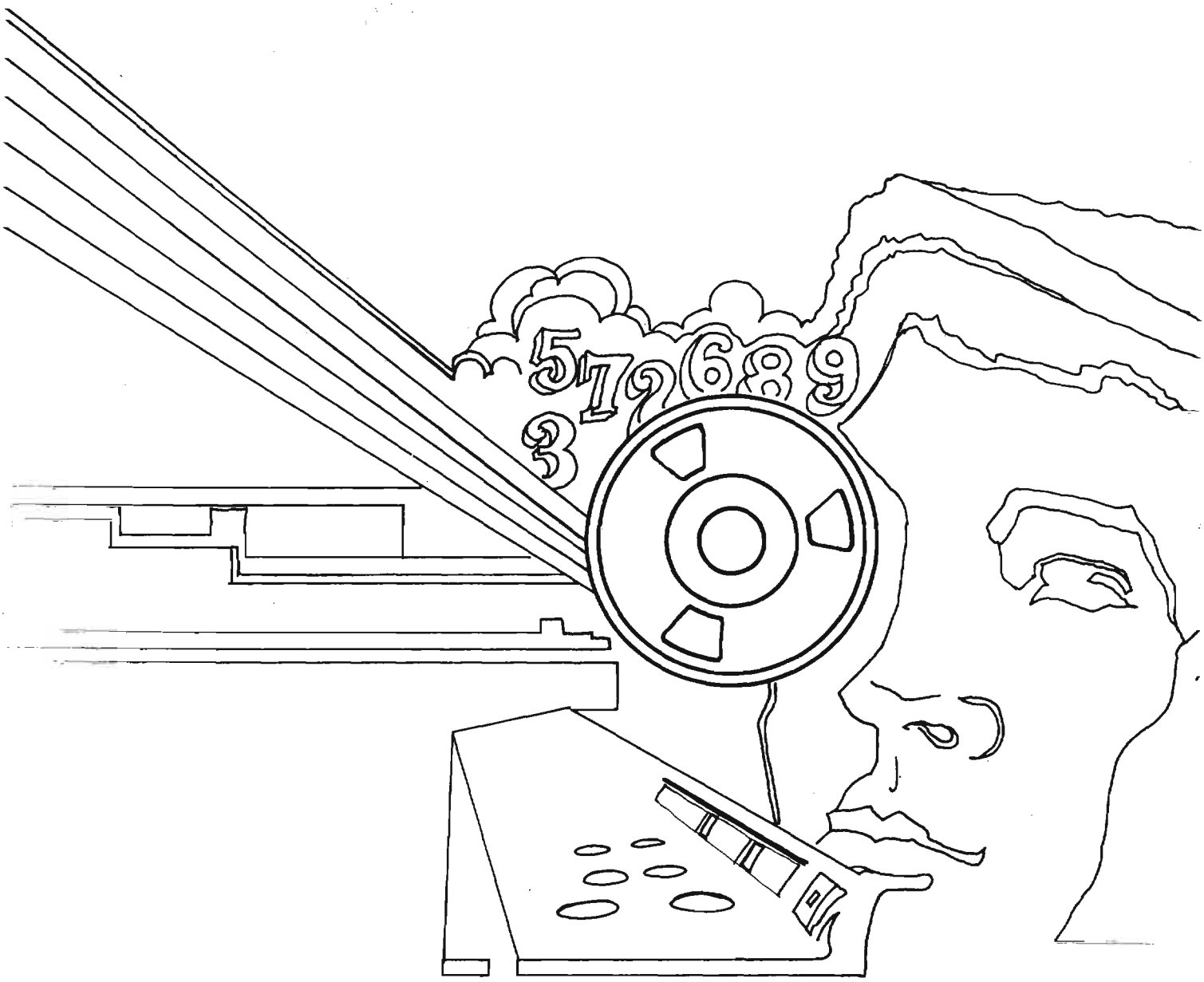
The following Prime Ministers or Heads of State were identified in Intelligence Product during the week of 25 April 1977. Can you associate the names and countries?

1. Amin
2. Asad
3. Bhutto
4. Boumediene
5. Castro
6. Daoud
7. Desai
8. Fahd
9. Fukuda
10. Geisel
11. Giscard
12. Hassan
13. Houphouet-Boigny
14. Lopez Portillo
15. Marcos
16. Mengistu
17. Mobutu
18. Morales Burmudez
19. Neto
20. Numayri
21. Nyerere
22. Qadhafi
23. Rabin
24. Ramgoolam
25. Sadat
26. Senghor
27. Siad
28. Soares
29. Suarez
30. Smith
31. Tindemans
32. Videla
33. Zia Urrahman

A. Afghanistan
B. Algeria
C. Angola
D. Argentina
E. Bangladesh
F. Belgium
G. Brazil
H. Cuba
I. Egypt
J. Ethiopia
K. France
L. India
M. Israel
N. Ivory Coast
O. Japan
P. Libya
Q. Mauritius
R. Mexico
S. Morocco
T. Pakistan
U. Peru
V. Philippines
W. Portugal
X. Rhodesia
Y. Saudi Arabia
Z. Senegal
a. Somalia
b. Spain
c. Sudan
d. Syria
e. Tanzania
f. Uganda
g. Zaire

Answers next month.

~~(CONFIDENTIAL)~~


5726893