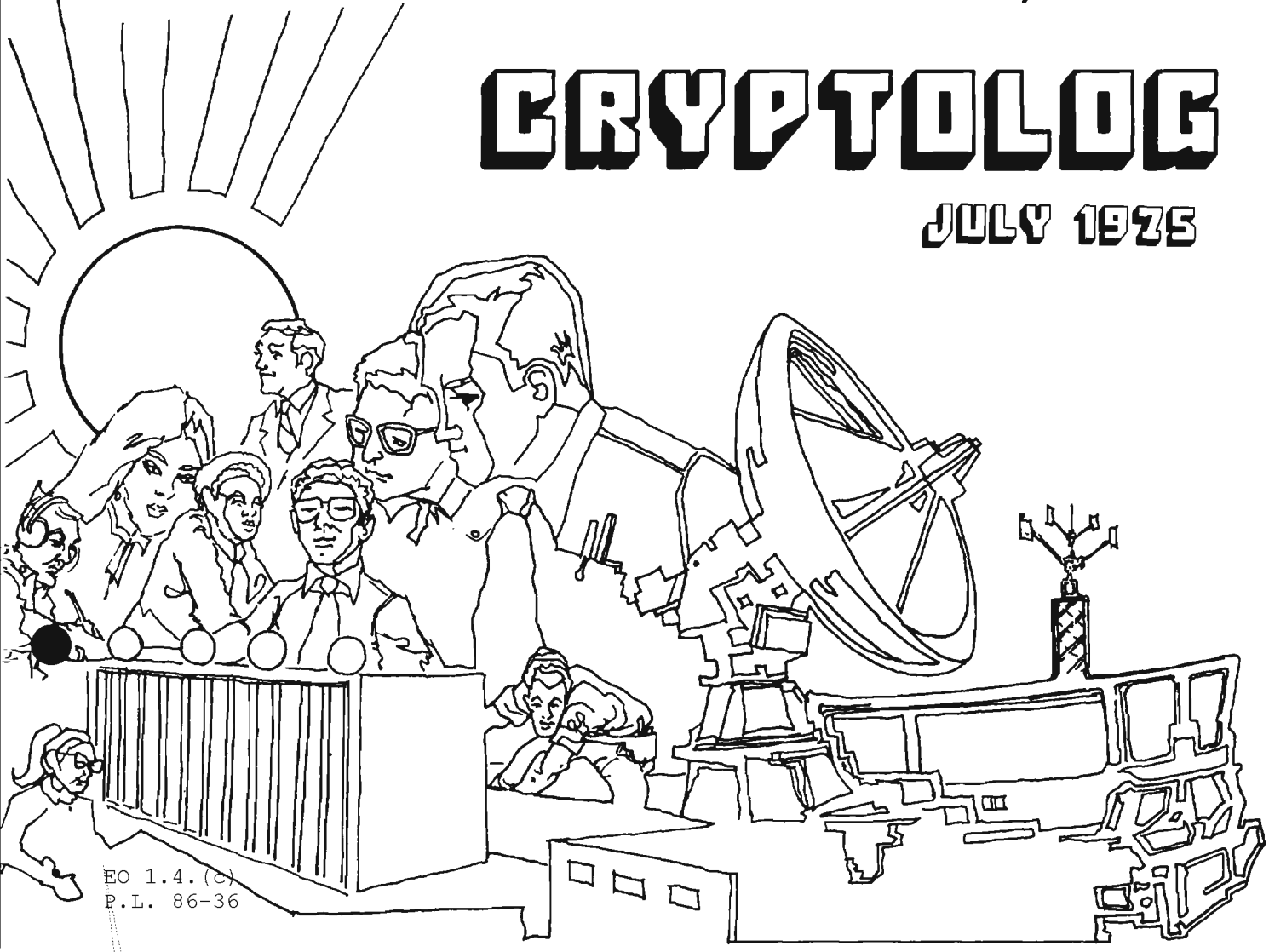
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JULY 1975



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

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

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

~~TOP SECRET~~

CRYPTOLOG

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

VOL. II, NO. 7 JULY 1975

PUBLISHER WILLIAM LUTWINIAK

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

~~TOP SECRET~~

~~TOP SECRET UMBRA~~

THE WARSAW PACT

[redacted]

[redacted]

P.L. 86-36

In recent years the Warsaw Pact has recognized the need for [redacted]

[redacted]

~~TOP SECRET UMBRA~~

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

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

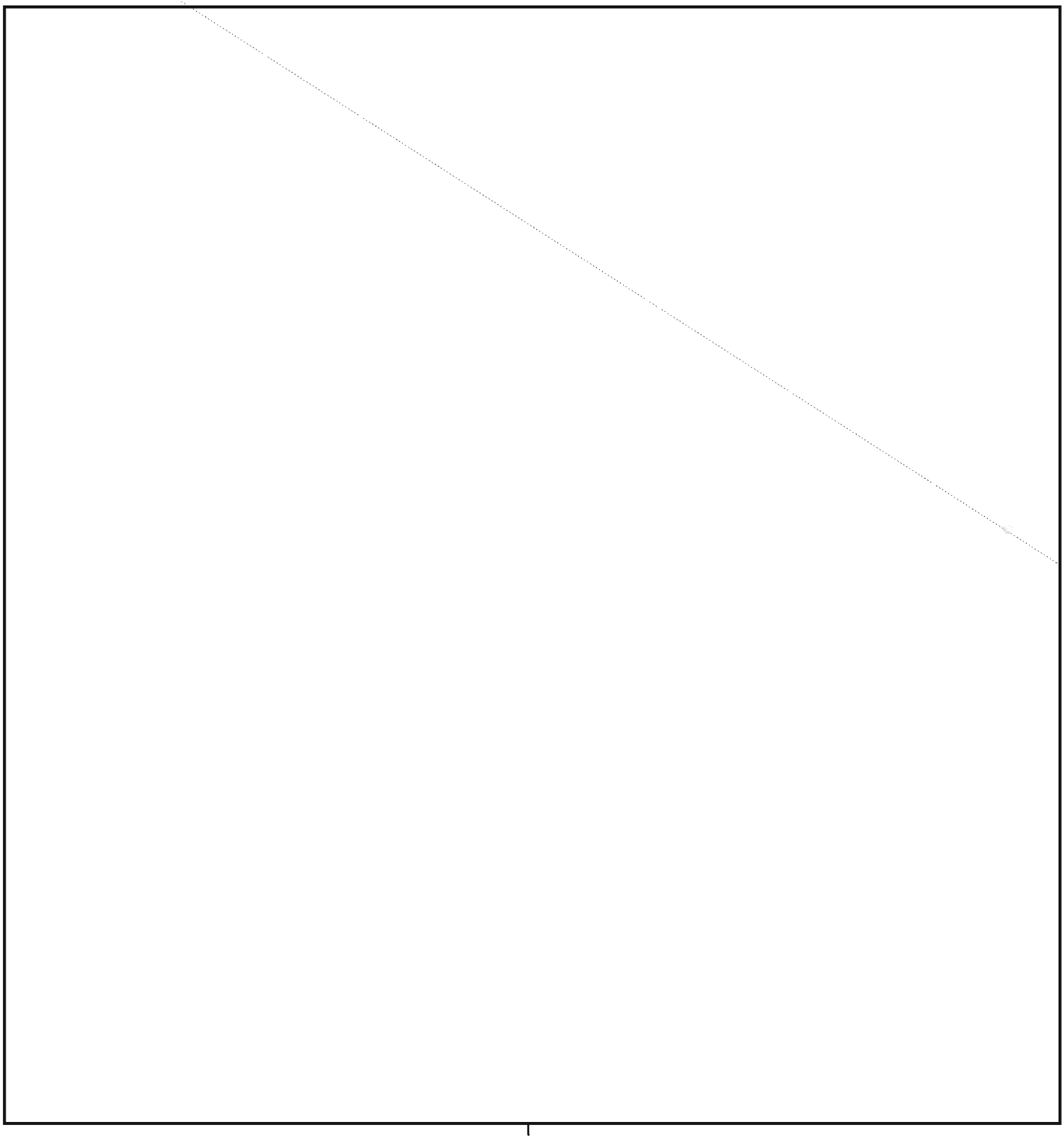
~~CONFIDENTIAL~~

T Y G S
SOO MANX FARBLER
A Moral Tale for Cryptanalysts

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

By [redacted]

P.L. 86-36



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

"RE-PSYCHLING" THE CODE CLERK

By [redacted]

P.L. 86-36

[redacted] *who is currently working* [redacted] *submitted the following response to the editor's invitation to "match" Mr. Callimahos' WWII observations in the April 1975 issue.*

Throughout the 1960's, the Vietnamese Communists were straightforward in their cryptographic habits and could be relied upon to be fairly secure [redacted] However, the VC code clerks, not unlike their Japanese counterparts in WWII (as discussed by Mr. Callimahos), had a peculiarity that gave the cryptanalyst that helpful boost.

In 1968 the VC began a gradual change from [redacted]

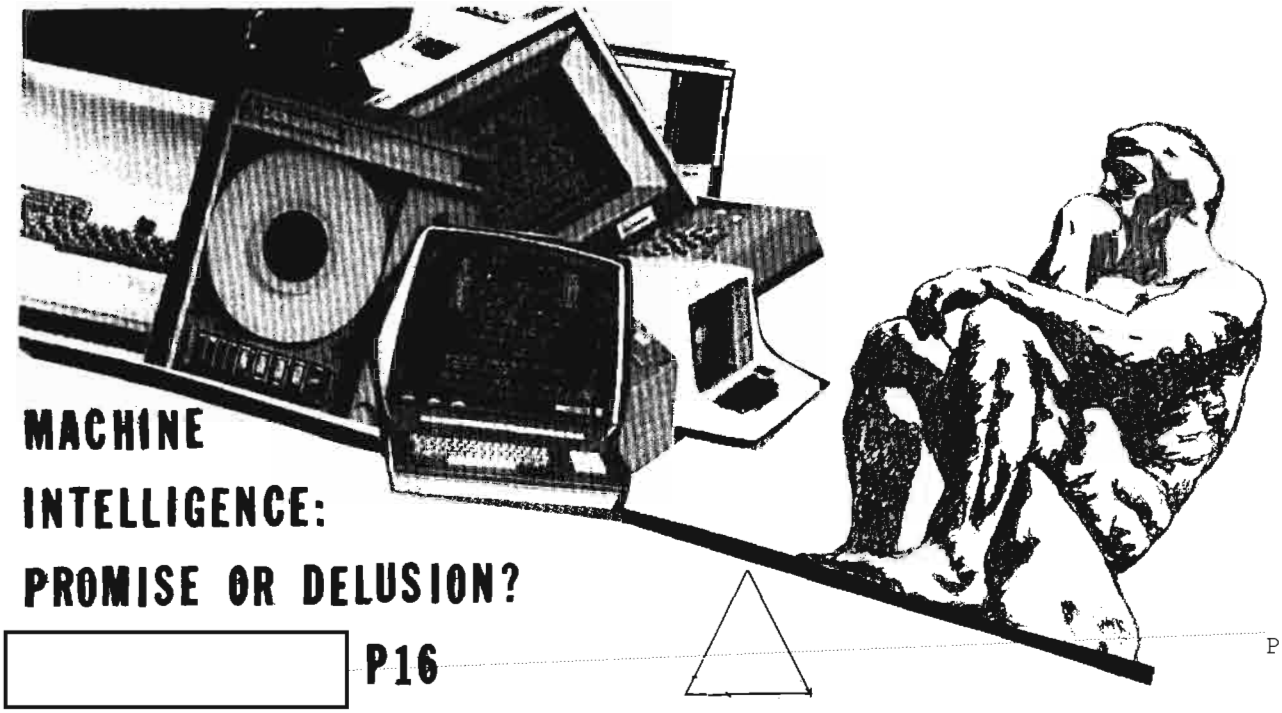
While there were indeed other features exploited by those engaged in the long-term, in-depth analysis of these communications, this particular one proved especially interesting to those of us engaged in the initial analysis of [redacted]

* * * * * * *

Solution to [redacted] Radiotelephone [redacted] in June 1975 issue.

[redacted]

Puzzle solution is ~~SECRET SPOKE~~



MACHINE INTELLIGENCE: PROMISE OR DELUSION?

[redacted] P16

P.L. 86-36

The following paper was written as part of a larger project that will include a selective review of ARPA-funded Artificial Intelligence research since 1967, in the light of the criticisms raised by Dreyfus and others. The results of this study will be published as a P1 Report in the near future.

> *What Computers Can't Do*, Hubert L. Dreyfus. Harper and Row, New York, 1972.

Hubert Dreyfus is a professional philosopher who has been a persistent gadfly to Artificial Intelligence (A.I.) researchers for several years. He published an earlier, strongly critical paper (Dreyfus 1965) whose points were all promptly and emphatically brushed aside by spokesmen for the A.I. community. Now he has written a book which, I believe, cannot and should not be so summarily dismissed by any thinking person, whatever his attitude toward computers.

For those readers who may not be familiar with that branch of computer science called Artificial Intelligence, it involves the attempt to program or build a digital computer capable of producing behavior that a human being would accept as truly intelligent. A.I. researchers have been trying, with varying degrees of success, to get computers to do such things as playing chess and Go; proving logical and mathematical theorems; understanding and translating written and spoken language; controlling a robot vehicle or an artificial arm and hand; perceiving and understanding visual scenes and patterns; and carrying out a sensible dialog with a human being on a topic of interest and importance. An excellent recent book that tells the story of A.I. from the point of view of a prominent worker in the field is Michie (1974). Unlike so much writing on technical topics, it is clear, readable, concise, and even enjoyable, and I strongly recommend it to anyone interested in a good survey from a friendly position.

Dreyfus presents a strong and well-reasoned claim that we will never be able to get digital computers to do any of the above-mentioned kinds of intelligent things nearly as well as people do them. He shows quite convincingly that the research he has reviewed, covering the years 1957 through 1967, has failed in all but a few relatively simple, highly formal and restricted tasks. He bases his case on purely philosophical grounds, on logic, and on a demonstration of the essential inadequacy of those often unspoken assumptions about the brain, the mind, human knowledge, and the nature of reality that underlie not only A.I. research, but in fact our whole Western scientific world-view.

Intelligent human activities are assigned by Dreyfus to four classes:

> *ASSOCIATIONISTIC ACTIVITIES*, innate or learned by repetition, such as memory games, maze problems, word-for-word substitution, and responses to rigid, unvarying patterns or stimuli.
>
> *SIMPLE FORMAL ACTIVITIES*, learned by rule, such as simple games (Nim, Tic-tac-toe), simple combinatorial problems,

mechanical theorem proving, and recognition of small sets of clear-cut patterns (e.g. typed character fonts).

COMPLEX FORMAL ACTIVITIES, learned by rule and practice, such as "noncomputable" games (chess, Go), complex combinatorial problems, nonmechanical theorem proving, and recognition of complex patterns in noise.

NONFORMAL ACTIVITIES, learned by example and insight, such as "ill-defined" games (riddles), open-structured problems, translation of natural language, and recognition of varied and distorted patterns such as speech.

A digital computer program, as Dreyfus readily admits, can carry out activities in Classes 1 and 2 quite adequately and even well. Class 3 activities are theoretically capable of being spelled out in a set of instructions, but in practice the resulting description is far too long and complex for brute-force implementation in any existing or presently conceivable computer. These activities are apparently accomplished by people through the use of powerful conceptual shortcuts and insights ("heuristics") which provide an immediate and dramatic reduction in complexity. While Dreyfus does not commit himself on the question of how far computers can go in "heuristic" attacks on Class 3 problems, his tone is decidely pessimistic. Activities in Class 4 are in a completely different world, Dreyfus claims, separated from Classes 1 through 3 by a major discontinuity that cannot be bridged by any computer program. These activities are inherently indescribable in terms of any formal language (such as mathematics, logic, and programming languages), and hence *cannot* be programmed. They exist at a level totally outside of, or prior to, the reasoning, digital, linguistic, description-generating capacities of our minds.

What picture of the world permits A.I. researchers, in the face of frequent setbacks, to remain so confident that computers can reproduce human intelligence? In studying this question, Dreyfus makes some of his most provocative and interesting points. He eloquently illuminates the philosophical bases of modern science, technology, computer science, and industry, and reveals the assumptions and biases culminating in the methods of A.I. research. Tracing this cast of thought back to Plato, he characterizes it thus: "...what cannot be stated explicitly in precise instructions -- all areas of human thought which require skill, intuition, or a sense of tradition -- are relegated to some kind of arbitrary fumbling" (p. xvi). He finds it again in Hobbes' *Leviathan:* "When a man *reasons,* he does nothing else but conceive a sum total from addition of parcels, ... for REASON ... is nothing but reckoning..." (p. xvii). He concludes that "Western thought has already committed itself to what would count as an explanation of human behavior ... a theory of practice which treats man as a device, an object responding to the influence of other objects, according to universal laws or rules" (p. 144). He states the following stern judgment upon this philosophy: "...the goal of the philosophical tradition embedded in our culture is to eliminate all risk: moral, intellectual, and practical."

Dreyfus points out that this reductionist viewpoint on the nature of man and human intelligence, however ordinary and familiar it may sound to us, is only one possible viewpoint, and has led us to make some assumptions which are not justified outside the realm of physics and the "hard" sciences. He makes explicit four major assumptions underlying A.I. research in particular:

A BIOLOGICAL ASSUMPTION, that the human brain, at some basic physiological level, employs discrete values in the same way as a digital computer;

A PSYCHOLOGICAL ASSUMPTION, that the human mind "can be viewed as a device" operating on discrete bits of information according to formal rules, again like a digital computer;

AN EPISTEMOLOGICAL ASSUMPTION, that all knowledge can be formalized," and "whatever can be understood can be expressed in terms of logical relations";

AN ONTOLOGICAL ASSUMPTION about the nature of reality and basic to the other three, that "all relevant information about the world, everything essential to the production of intelligent behavior, must be analyzable as...a set of indifferent, passive facts, each logically independent of all the others."

If these mechanistic assumptions are not adequate to explain human behavior, then what are the capacities that permit people to do the intelligent things that computers cannot do? Dreyfus suggests an attractive alternative viewpoint based on Gestalt Psychology and the philosophical school of Phenomenology -- fields which his arguments should motivate any thoughtful reader to examine more closely. He makes a good case for a primary nondigital or "analog" capability, which allows the human mind to accomplish what it does. To paraphrase Dreyfus' definitions, a digital device represents data by discrete states (e.g. a switch assuming two or more distinct positions), and gets a result by counting. An analog device uses physical quantities (voltage, duration, angle of rotation of a disc), proportional to the value to be represented, then combines these quantities physically and measures the result. He shows that many neurologists and psychologists lean increasingly toward postulating analog devices in the human brain, and a continuous, field-like mode of functioning in human perception and cognition.

Four major nondigital features are presented by Dreyfus as characteristic of, and essential to, human information processing. These are:

FRINGE CONSCIOUSNESS -- the ability to use the background structure of a gestalt within which objects of our conscious attention are embedded. For example, a chess player says of his opponent, "I notice that one of his pieces is not defended, the rook..." In so doing, he does not resort to a systematic inventory of all the pieces on the board, but perceives a high-level field of relationships all at once, at a glance, crystallizing around a single piece -- the rook -- to which his eye is drawn.

AMBIGUITY TOLERANCE, or *CONTEXT DEPENDENCE* -- the ability to deal with ambiguous situations without having to transform them by substituting a precise description. People are able to use complex, coordinated schemata of knowledge about the world, stored and retrieved in some unknown manner, to rapidly resolve ambiguity in any given situation.

ESSENTIAL-INESSENTIAL DISCRIMINATION, or *INSIGHT* -- the ability to select a constantly changing set of things in our cognitive world as important to us with respect to our current and ever-changing motivations and goals. This is, in fact, what a human programmer does for the computer when he plans a program: he prearranges matters so that only those objects and relations needed for the purpose of the program are singled out and described, leaving the machine with a simple formal (Class 2) problem to solve.

PERSPICUOUS GROUPING -- the ability to perceive structured wholes as elements, rather than exhaustively and mechanically searching through lists that spell out a higher-level pattern in terms of many atomic traits. Psychologists have been learning more about human and animal perception, and are demonstrating that we do not build up percepts additively from tiny units such as individual points of light on the retina. Instead, the visual mechanism works with much more complex elements: edges, moving horizontal or vertical bars, small or large areas of light or dark that expand or contract, etc. We are capable, further, of recognizing distorted or varying patterns directly, and not by successively and mechanically transforming what we see until it matches a stored template or ideal form. We can even recognize a "family resemblance" among objects, even though they may have no explicit single trait in common.

Dreyfus' last and most interesting point about human information processing concerns the crucial importance of our bodies and bodily skills, the fact that, "living in our bodies we have built up a motor space..." An essential difference between metal machines and "meat machines" (as some over-enthusiastic modern reductionists have called us), is that we are "embodied" in a way no digital computer can ever be. Thus, our experience of a tool we are using is essentially different from our experience of an object; the tool is an extension of our body, a "transparent access to the objects we touch with it." Dreyfus suggests that we learn to speak our native language in the very same way -- as a bodily skill (and this would certainly explain the relative difficulty of second-language learning, which must be accomplished long after our basic body schemata have been formed).

Thanks to these bodily skills, man is "at home in his world, has it comfortably wrapped around him, so to speak. Human beings are somehow situated in such a way that what they need in order to cope with things is distributed around them where they need it, not packed away in a trunk full of objects, or even carefully indexed in a filing cabinet. This system of relations which makes it possible to discover objects where they are needed is our home or our world" (p. 172). It is instructive to contrast our experience when we are forced to orient ourselves in a world where we are not yet "at home" -- learning a new game or skill, finding our way about under water or in a foreign city. For a while, in the new situation, we too must operate hesitantly, slowly, formally, and often quite ineffectually, like the digital computer.

Dreyfus is highly pessimistic about the degree of success attainable by A.I. researchers who base their work upon the set of assumptions he criticizes. He concedes that an "artificial embodied agent" might someday be developed, but only if it relied extensively on analog techniques not presently imaginable to us. He very briefly considers the possibility of a learning device, which might start out with an initial minimal "body schema" like that of a newborn baby: a tiny store of "facts" and some basic motivations as elementary as the baby's predilection for "nipples and smiles." It might then build up a respectable "world" in time under the tutelage of patient human mentors. I do not feel that he accords enough serious consideration to this possibility, which seems well worth pursuing (and, in fact, will undoubtedly be pursued in some form within the next few years). He dismisses it rather arbitrarily in the following words: "Computers can only deal with facts, but man -- the source of facts -- is not a fact or set of facts, but a being who creates himself and the world of facts in the process of living in the world... There is no reason to suppose that a world organized in terms of these fundamental human capacities should be accessible by other means" (p. 203).

The patient reader, having stayed with this review this far, may be asking himself, "Why should I care? What does all this matter to me, in my job or anywhere else?" First, I would like to convince you, the reader, that it all matters quite a lot to us, both as NSA employees, and also, in a wider context as thinking people caught up in the frenetic and often inhumane activities of a Western industrial society. We care at NSA because many of the things we will need to do in the next five or ten years will undoubtedly call for solution of some problems verging on the realm of Artificial Intelligence. Our requirements have always pushed the "state of the art" to its limits, and they may soon include such things as speech and language understanding, optical pattern recognition, and the handling of very large, organized knowledge bases. We are faced with essentially the same barriers of size and complexity as are plaguing A.I. research.

ARPA, the Advanced Research Projects Agency of the Defense Department, is in fact the major source of funding for A.I. research, and is at present under attack from several directions because its projects are not considered to be "paying off" as rapidly as they should be for the expenditures involved. The more pragmatic of Dreyfus' criticisms, even though they may be dismissed out of hand by A.I. workers, are echoed by others not so easily brushed aside, for example J. Lighthill (1973) speaking for the Science Research Council in England. If enough critics succeed in discouraging ARPA research, and A.I. work in general, some of the potential benefits for NSA that might have been around the corner may never materialize. One promising spin-off of A.I. technology, possibly within the next five to ten years, is a "super-intelligent terminal" based on a number of techniques whose feasibility has been demonstrated by current ARPA-funded projects. Such super-terminals might make our jobs a lot easier in the near-future world of computer networks and agglomerations of data bases.

Finally, I feel that, aside from the immediate practical feasibility or consequences of A.I. research, all of us should care about the more basic points Dreyfus has made. Our socieity bases all of its ways of doing things on the set of assumptions whose limitations Dreyfus so clearly exposes. A number of other books have been appearing lately that attack the scientific world-view and its philosophic bases; two that I strongly recommend to the brave reader are Roszak (1972) and Schumacher (1973). It is easy to dismiss such writers as irrational, romantic, impractical, or mystical. I find myself, somewhat to my sorrow, agreeing wholeheartedly with most of their fundamental points of view. I still cannot accept Dreyfus' pessimistic conclusion, that an "artificial embodied agent" or even, as a more immediately attainable goal, an "intelligent digital assistant," is forever impossible. I am also not convinced that such an undertaking must necessarily be a bad or perverse one, as Dreyfus obviously feels.

The criticism Dreyfus and others have raised should certainly not be used as an excuse to shut off A.I. research; neither should they simply be brushed aside. Instead, we should heed the clear warnings that our world is much too narrow, that we are in danger of leaving out all the truly important things, and that we must begin empirical explorations of some alternative approaches to human nature and human thought to supplement the digital computer model. In any case, it seems clear that the thoughtful reader, whatever his attitude toward computers and technology, can profit by conscientiously exploring Dreyfus' well-reasoned case for "What Computers Can't Do."

Dreyfus, Hubert L. (1965). *Alchemy and Artificial Intelligence.* RAND Corporation, Paper P3244 (AD 625 719), December 1965.

Lighthill, Donald (1973). "Artificial Intelligence: A General Summary," *Artificial Intelligence: A Paper Symposium.* Science Research Council Pamphlet, Science Research Council, State House, High Holborn, London, April 1973.

Michie, Donald (1974). *On Machine Intelligence.* Wiley, New York, N. Y., 1974 (Q335/M58).

Roszak, Theodore (1972). *Where the Wasteland Ends: Politics and Transcendence in Postindustrial Society.* Doubleday and Co., Inc., Garden City, N. Y., 1972.

Schumacher, E. F. (1973). *Small Is Beautiful: Economics As If People Mattered.* Harper and Row, New York, N. Y., 1973.

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

RAPIDTRAN

P.L. 86-36

G95

At the first meeting of the Crypto-Linguistic Association's newly-established Special Interest Group on Translation (SIGTRAN) on 22 January 1975, the guest speaker was [redacted] of B Group and his topic was "Free-Lance Translation."

During the course of his talk, he made the following comments: "The real truth on what you earn as a free-lance translator is not what you get per 1000 words. It's how fast you translate. If you write out everything in longhand, obviously you're not going to make much money. Even if you type your translation directly, you're not going to make much money."

This fiscal fact of life, plus "pressures at home," led him to an interesting solution. "I was forced to mechanize. And I soon found that you can double, triple, and quadruple your translating speed simply by reading into the dictaphone."

Then he added, "I have often wondered why people in this Agency who translate things that remain constant, [redacted] After getting good enough, the typist can even proof for you. I know of no instance in which that has been tried. I know of a number of specific areas where I believe it would work.

"While we do talk, and properly so, of the problem of having management understand us linguists, I don't know of any managers who have, as they perhaps should, challenged our production as linguists. If a linguist produces three translations or eight translations all day, the usual manager doesn't know enough about the linguist's problems or procedures so as to be able to make an effective judgment on whether that is a proper output in terms of time."

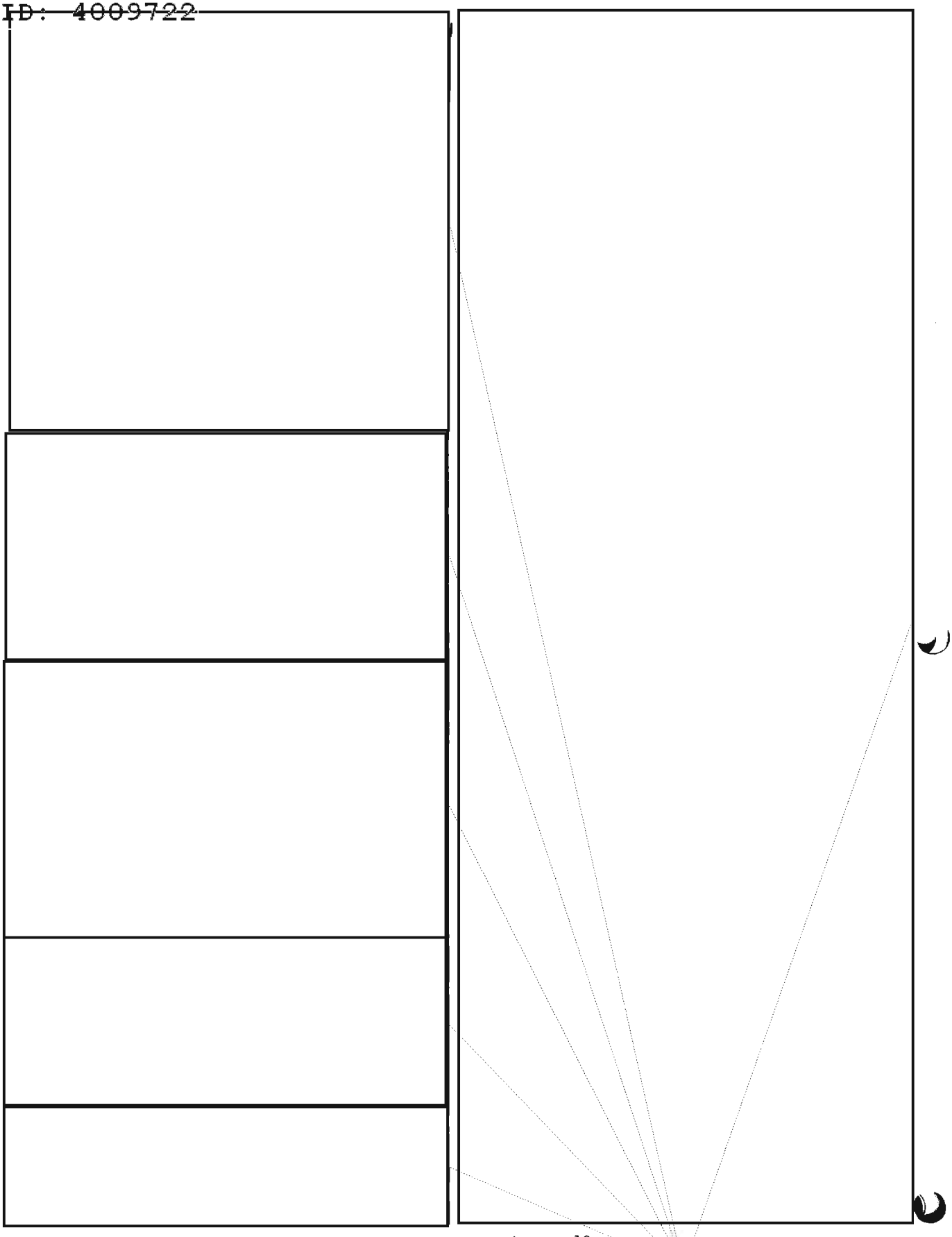
As the language coordinator for G9, the [redacted]

[redacted] I reacted to [redacted] refreshingly candid observations as though he had thrown down a gauntlet that we could not refuse to pick up. P.L. 86-36

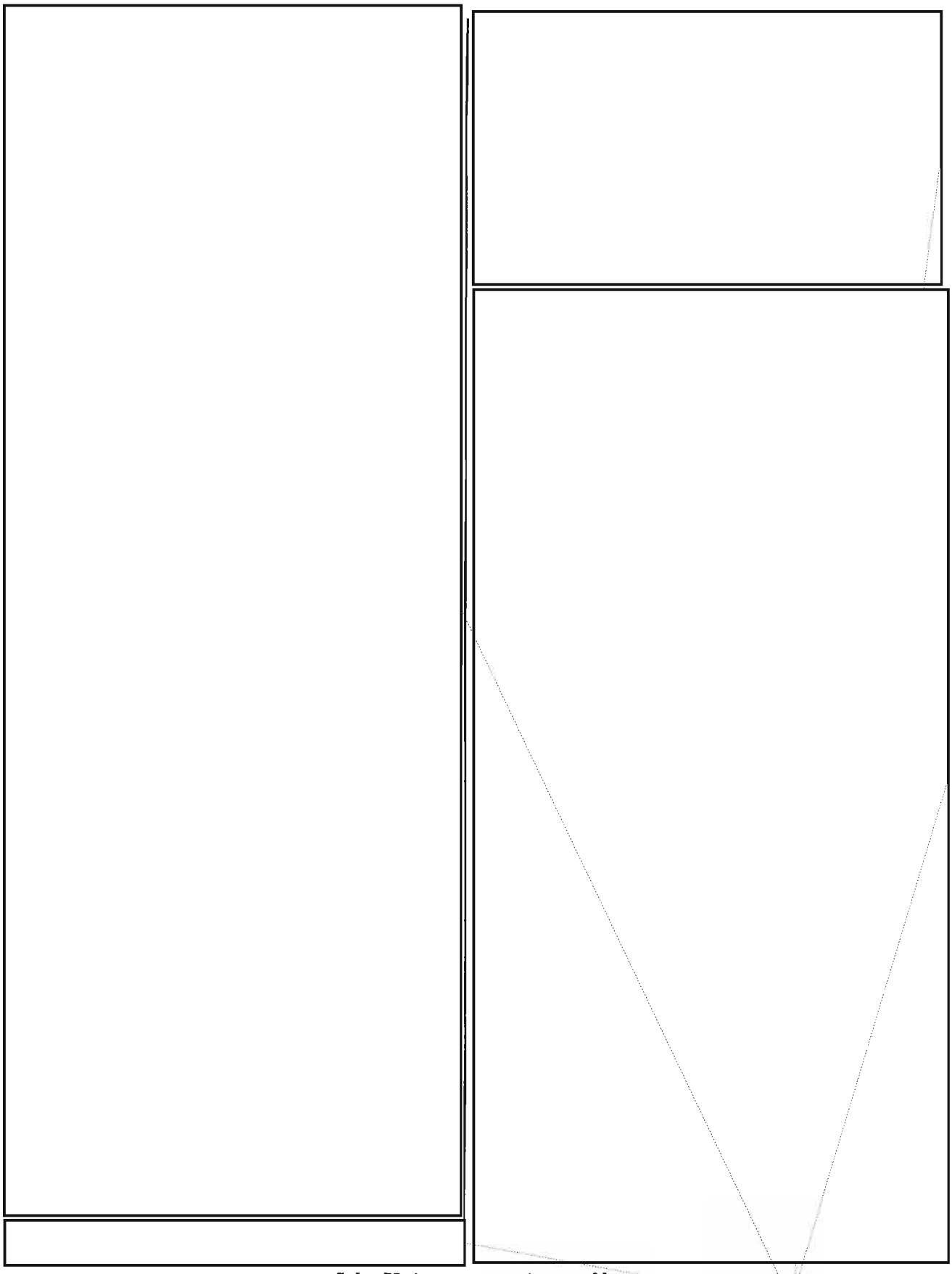
[redacted]

Freeing the SIGINT translator from the constraints of a pencil or typewriter was apparently attempted as early as 1946 by an enterprising Russian linguist by the name of Jack Gurin who was involved in the translation of [redacted] who decided to dictate his translations to a stenographer. He estimates that his output doubled the total achieved by the "traditional" method.

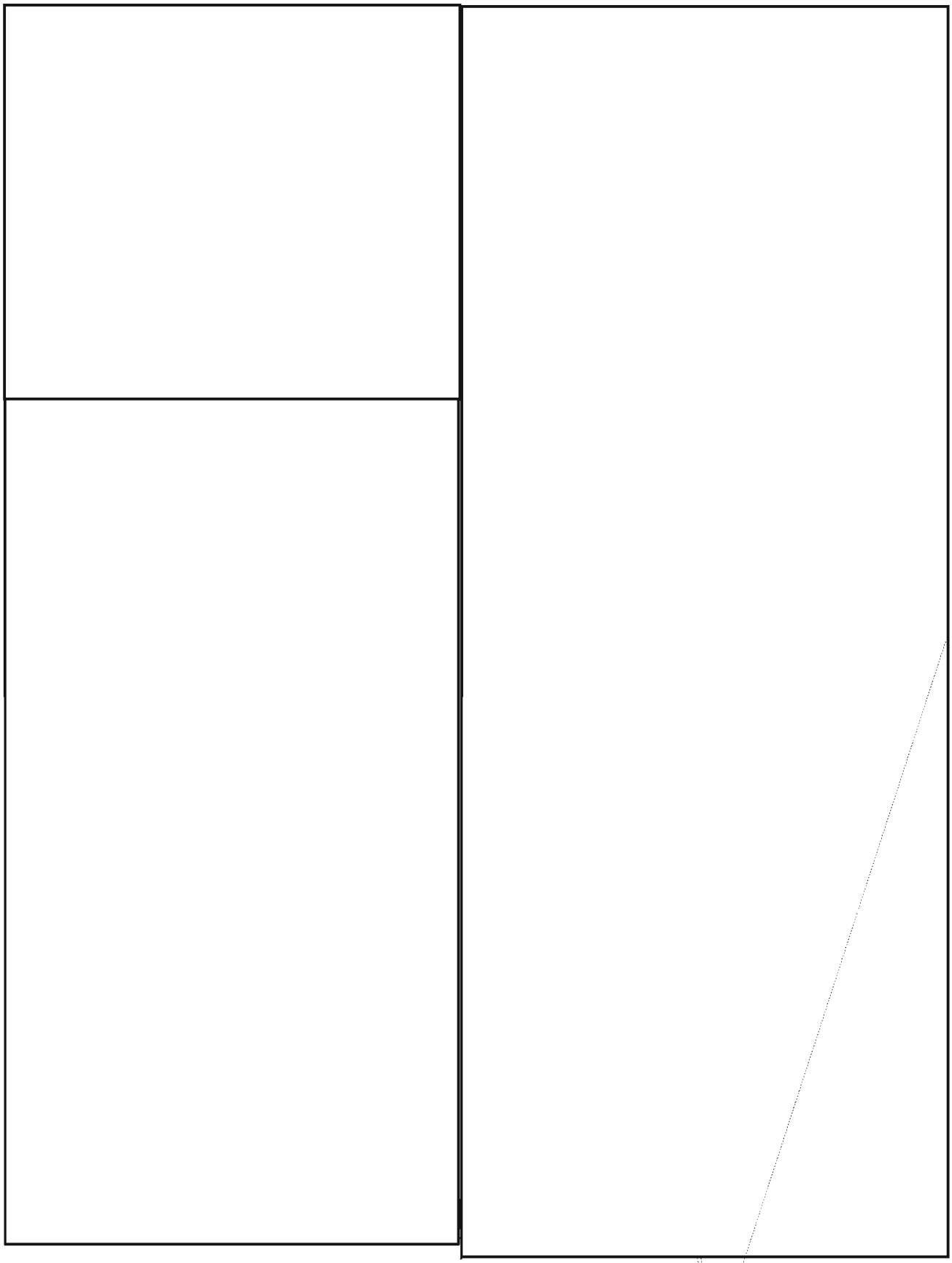
EO 1.4.(c)
P.L. 86-36



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



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



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

~~SECRET~~

NEWS BRIEFS FROM THE CMI AND CLA

At their respective annual banquets, held in May, the Cryptomathematics Institute and the Cryptolinguistic Association announced the following winners in their 1975 essay contests.

CMI Essay Contest

1st Prize ($100) -- [redacted] R51, "Cycles from Nonlinear Shift Registers" (UNCLASSIFIED).

2nd Prize ($50) -- [redacted] G93, "Linear Programming Applied to Manual Cryptosystems" ~~(TOP SECRET CODEWORD)~~.

3rd Prize ($25) -- [redacted] A54, "Symmetric Approximations to Boolean Functions" ~~(SECRET)~~.

CLA Essay Contest

1st Prize ($100) -- Doris E. Miller, P16, "Language and the COMINT Production Process" ~~(TOP SECRET CODEWORD)~~.

2nd Prize ($50) -- Emery W. Tetrault, P16, "U. S. Linguists and Language Capability Overseas" ~~(SECRET CODEWORD)~~.

3rd Prize ($25) -- Jacob Gurin, R54, "Examining Some Myths About Language" ~~(SECRET, HVCCO)~~.

Except for Mr. Gurin's article, which was published in *NSA Cryptologic Spectrum*, all the prize-winning articles were published in *NSA Technical Journal*.

P.L. 86-36

* * *

The CLA bestowed its Third Annual Sydney Jaffe Award upon [redacted] Chief, [redacted] Research and Support Organization). The citation reads in part: [redacted] total contribution to the large Russian language output of the Agency over the past 15 years is inestimable. He has insisted on maintaining the highest standards in language-based product in the face of a growing trend toward larger and more rapid production. At the same time he has moved to improve the rapidity of language support by mechanizing research files, combining them with those of collaborating centers, and preparing his own staff to deal with more difficult and more specialized language texts."

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

* * *

~~(SECRET -- HANDLE VIA COMINT CHANNELS ONLY)~~

¡CAMINO EN INGLÉS!

There are times when it is useful for analysts to scan the English meanings in a foreign-language glossary in order to find all the foreign terms relating to a given topic or set of topics. [redacted] For the off-line IBM-370 files, of which we now have a considerable number, a special program has been developed to provide a capability of this kind. The program retrieves and prints all entries whose English meanings contain one or more of a set of retrieval words specified by the user.

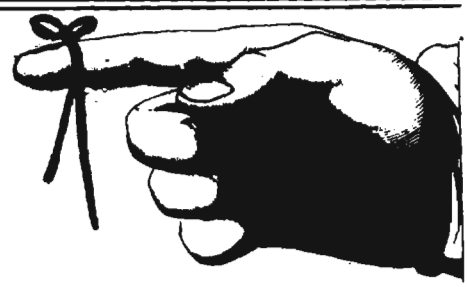
The program was developed in response to a request for any terms referring to various aspects of Electronic Warfare [redacted] The program can be run against any CAMINO file in the IBM-370 format. False hits can, in most cases, be eliminated by inspection of the full entry, and any remaining doubts can be resolved by the file executive. Users interested in trying out this English term retrieval capability are invited to contact [redacted] P16, x3045s.

~~(CONFIDENTIAL)~~

P.L. 86-36

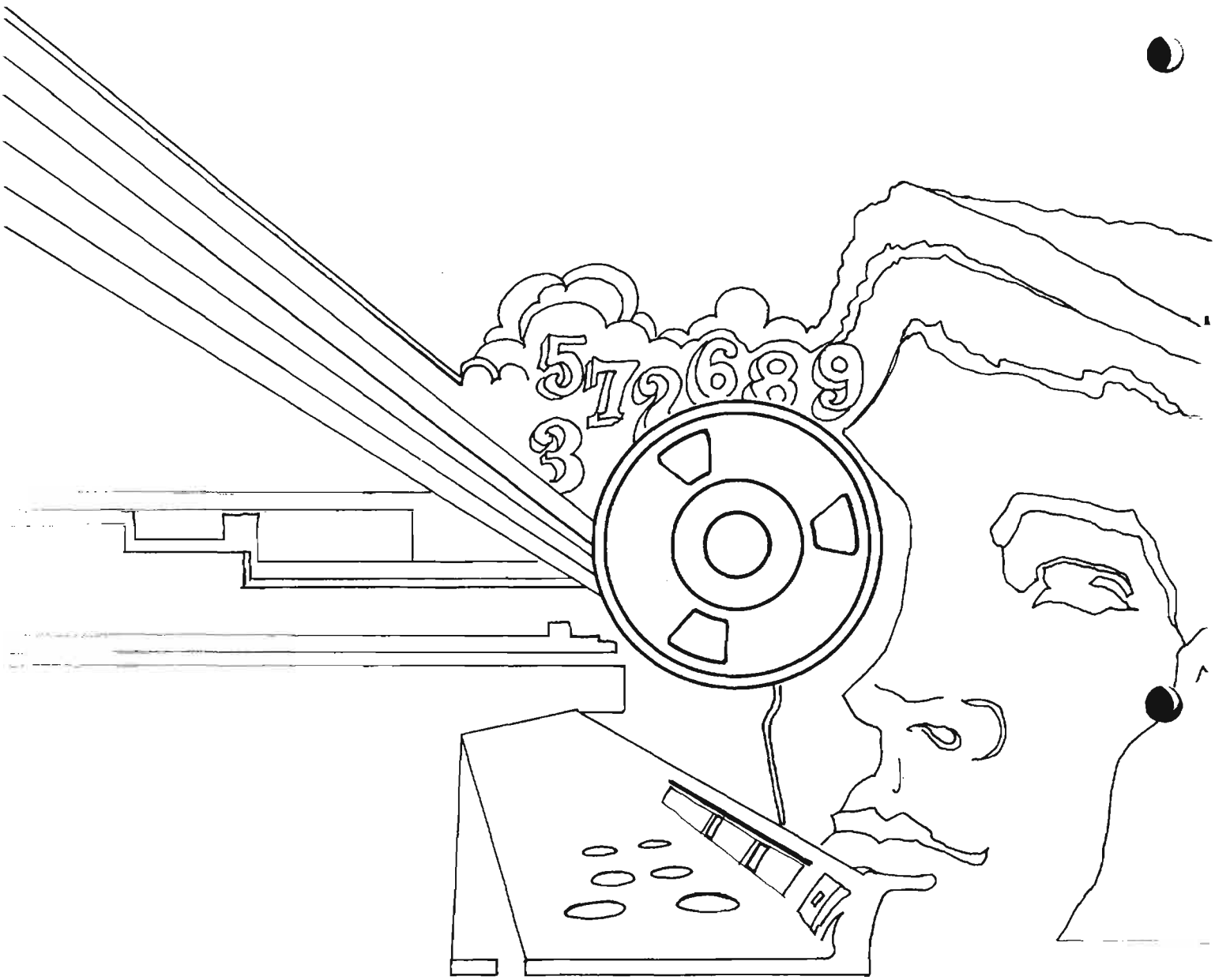
REMEMBER 15 AUGUST!

Not necessarily as the anniversary of the founding of Asuncion, Paraguay (1537), but definitely as the deadline for submitting your article to CRYPTOLOG for possible inclusion in the special "Vietnam Wrap-Up" issue to appear in October. Send your article to CRYPTOLOG Editor, P1. (U)



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

P1-JL 75-S3-24000


5179689
3