~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JUNE-JULY 1976

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

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

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

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

for the Personnel of Operations

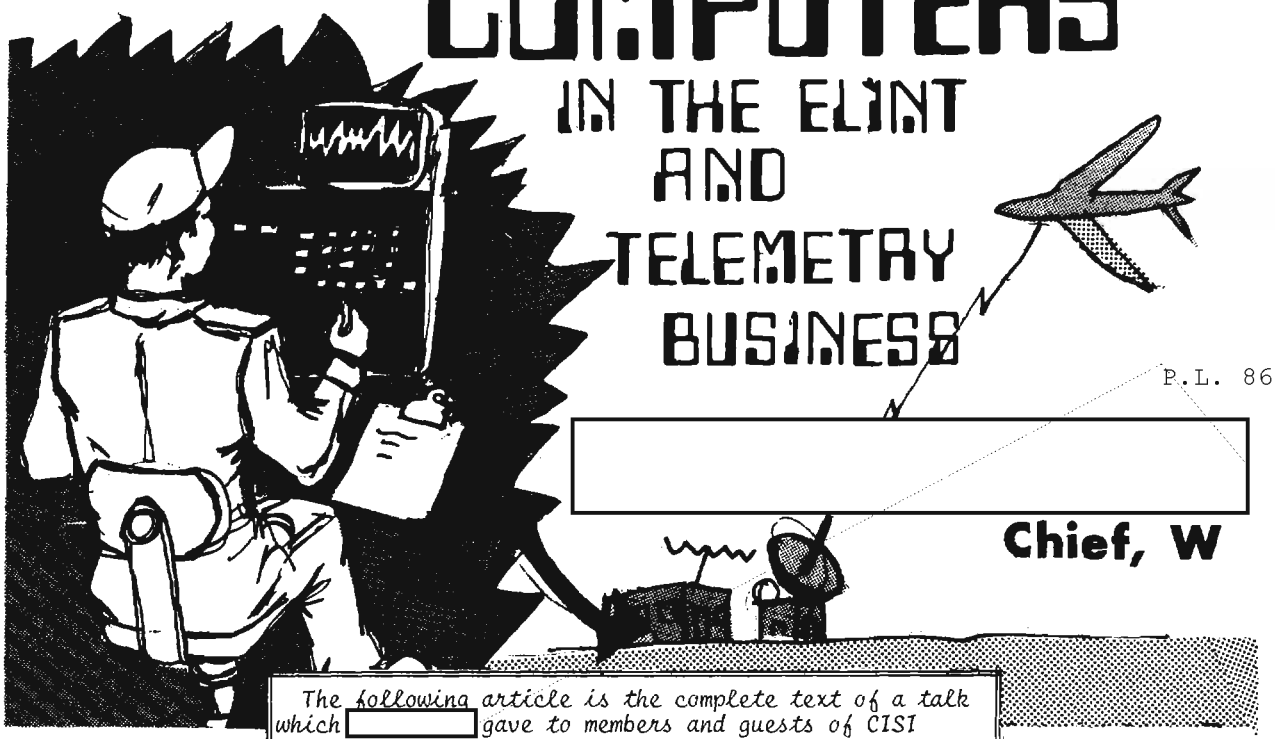
VOL. III, Nos. 6 and 7 JUNE-JULY 1976

PUBLISHER WILLIAM LUTWINIAK

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

~~TOP SECRET~~

COMPUTERS IN THE ELINT AND TELEMETRY BUSINESS



[redacted]

Chief, W

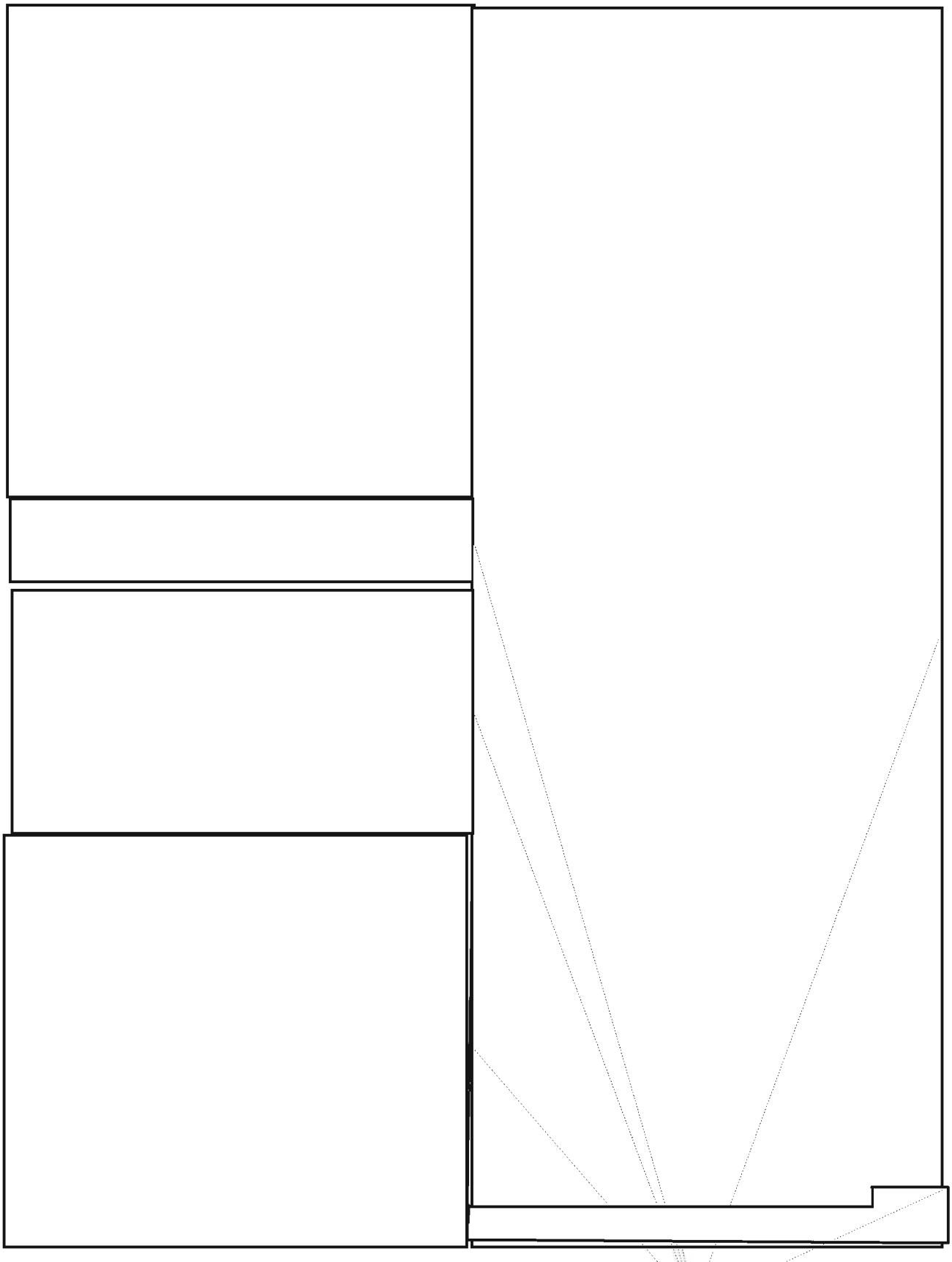
The following article is the complete text of a talk which [redacted] gave to members and guests of CISI (NSA Computer and Information Sciences Institute) in the Friedman Auditorium on 22 January 1976.

In order for you to calibrate what I have to say, I want to make it very clear that I am not a computer expert. I have never participated in the design of any computers, I have had little operational experience with the care and feeding of them, and I have never written software. But I have had the opportunity to help design and work with a number of systems that use computers in very important ways, and I am in a position now to affect the market for computers in the ELINT and telemetry business. I'll be directing my remarks at *uses*, not computers themselves.

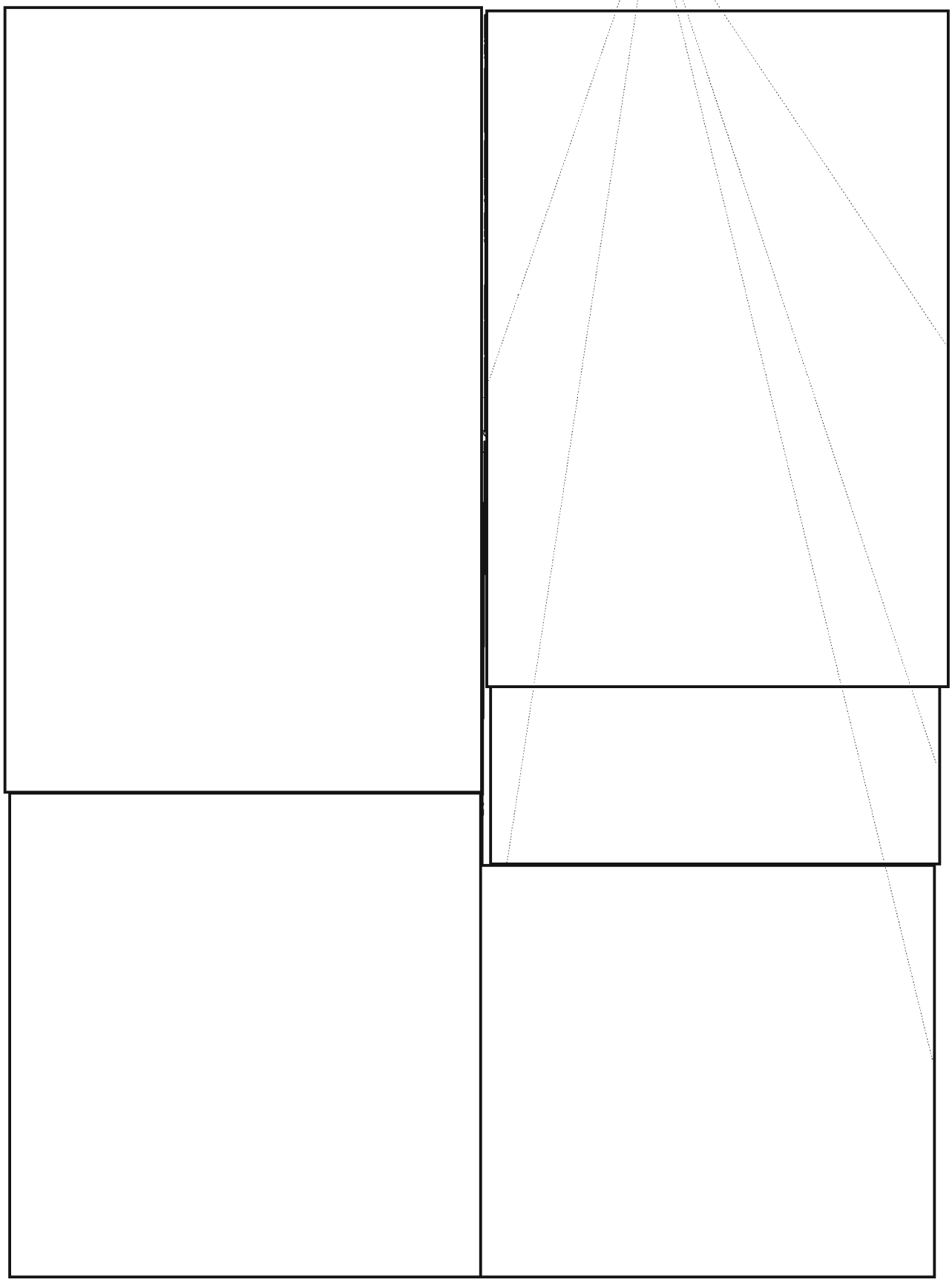
When you don't intend to say anything very profound (or may be afraid that you won't, although it is all that you know), you often call your talk or book an "Introduction to. . ." I've resisted that today, just to lure more of you here. But it was suggested to me that a brief introduction to ELINT and telemetry might be in order. I'll start with that and keep it *very* basic. Then I'll phase into the description of a current set of computer applications, and end with what I see as real trends in this area.

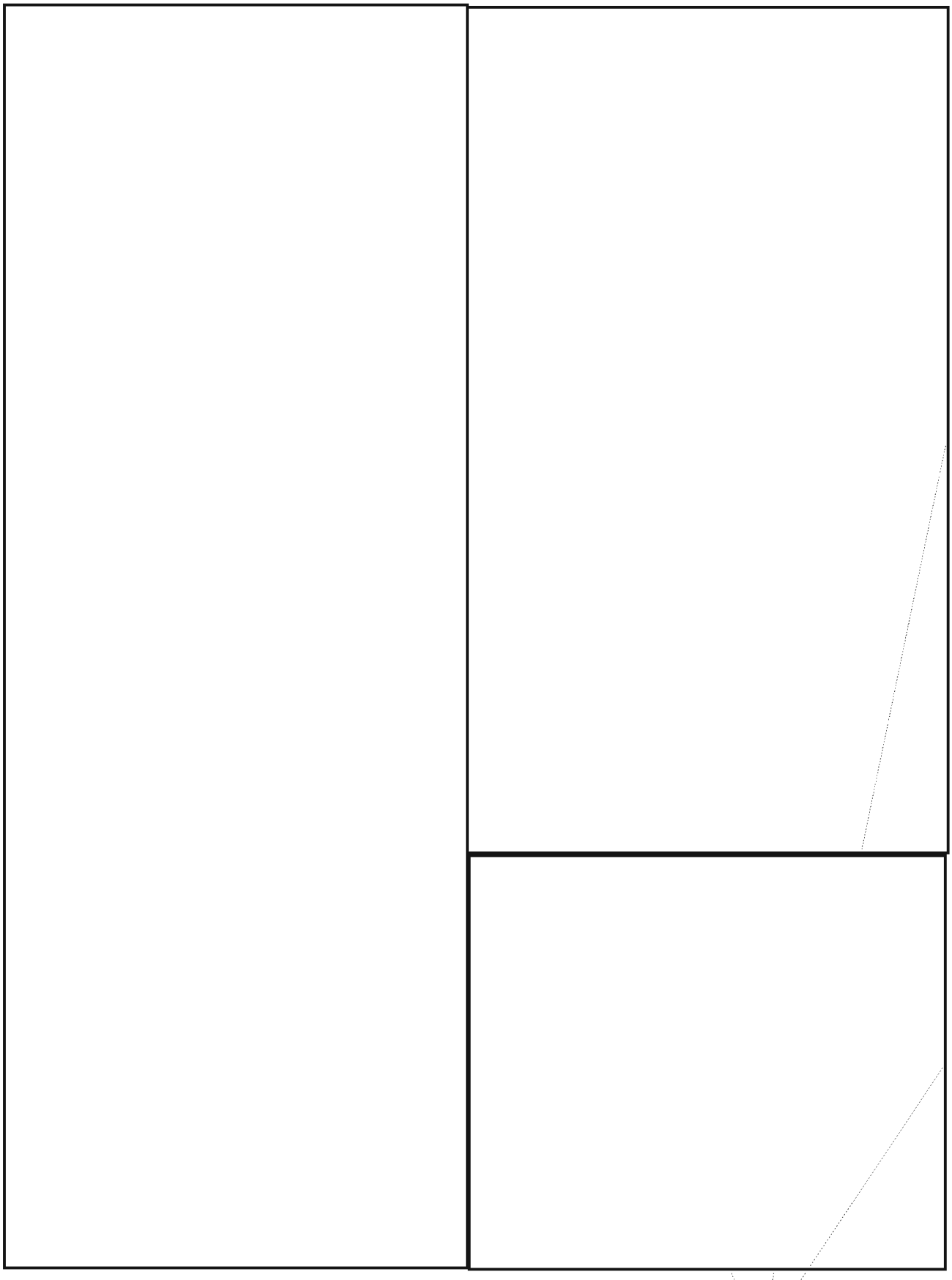
[redacted]

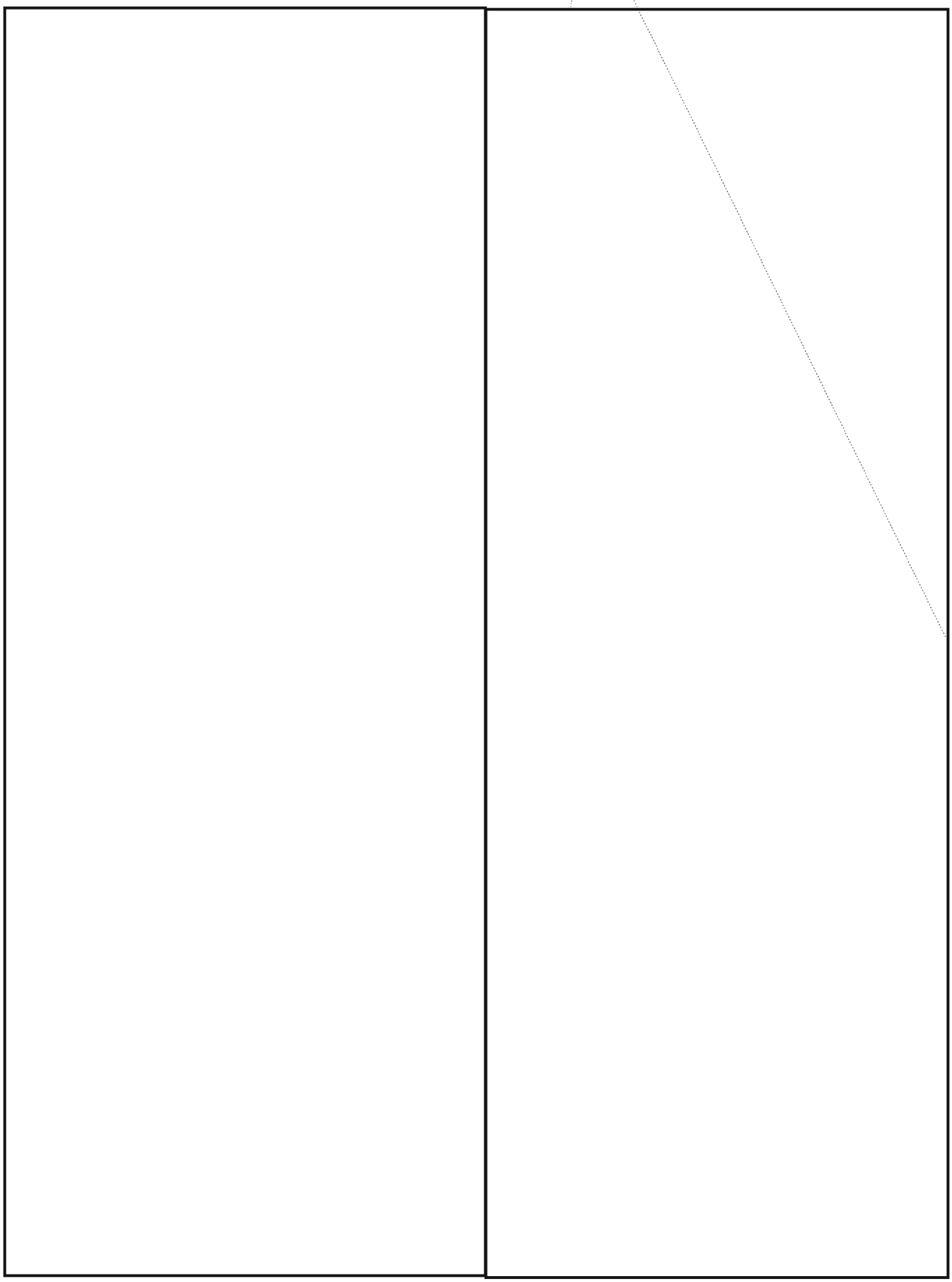
[redacted]

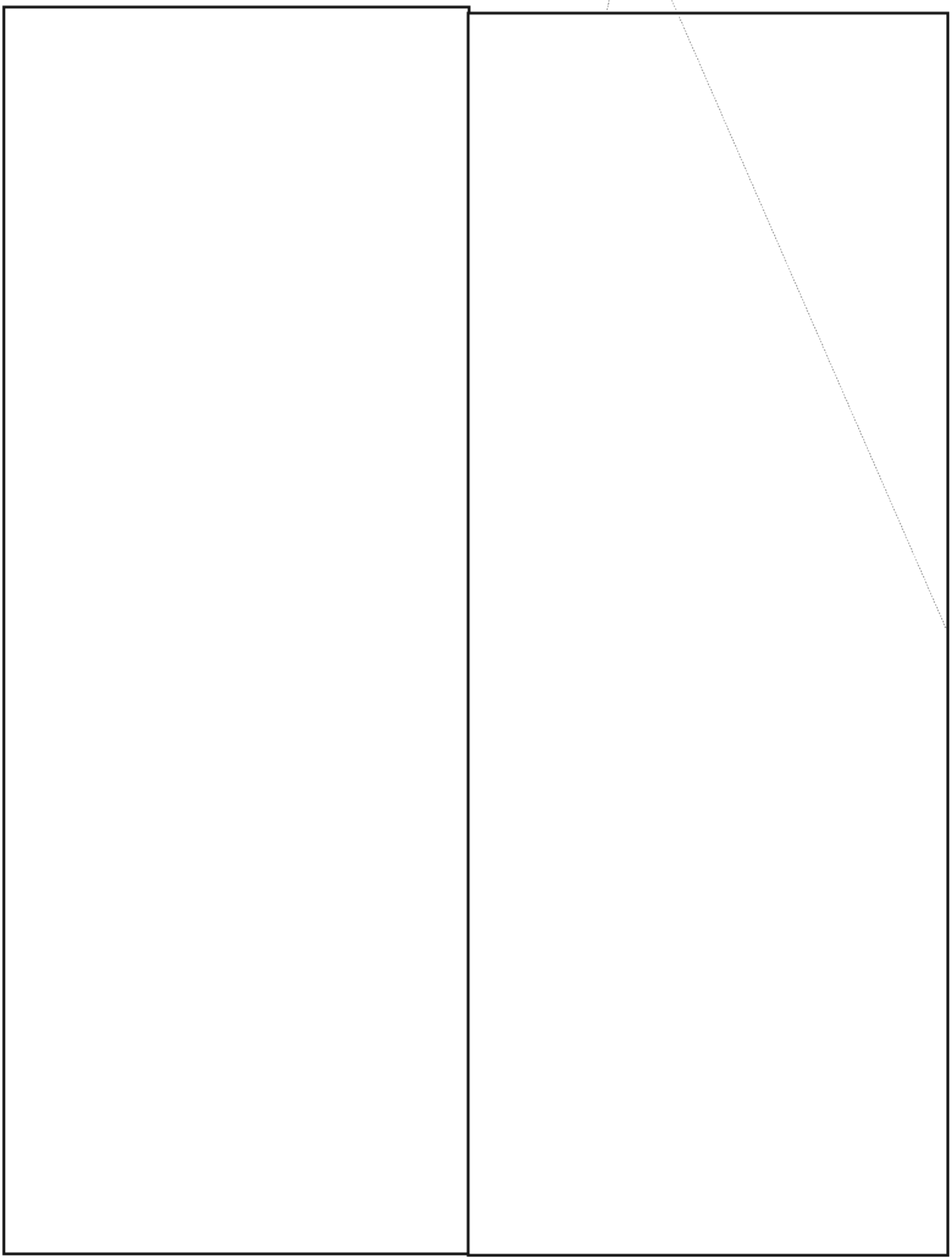


EO 1.4.(c)
P.L. 86-36









TOP SECRET

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

[redacted]

(TOP SECRET - HVCCO)

P.L. 86-36

"RIGHT ON, VERA!"

Vera Filby's article on radio deception, "How Do We Know It's True?" (CRYPTOLOG, February 1976), has elicited much comment here at the Agency, and has even prompted a couple of people to put their thoughts on paper (see "On Being Truthful," by [redacted] CRYPTOLOG, April 1976, and "Some Principles of Cover and Deception," by [redacted] CRYPTOLOG, May 1976). The following message from Germany indicates that the subject of radio deception is indeed, as Ms. Filby pointed out, one of vital concern to other Agencies as well as our own. MGEN Smith has granted his permission to publish his remarks in full.

Ed.

FM: NCEUR [redacted] EO 1.4.(c) P.L. 86-36

TO: NSOC

(E12, DDF, A, A7, A8)

FOR VERA FILBY FROM [redacted] P.L. 86-36

SUBJ: HOW DO WE KNOW IT'S TRUE?

REF: [redacted]

B. CRYPTOLOG MAGAZINE, FEBRUARY 1976, PAGE 6

1. VERA, YOUR ITEM IN THE FEBRUARY 76 CRYPTOLOG RECEIVED MUCH INTEREST HERE AT STUTTGART. BY COINCIDENCE (UNLESS YOU PLANNED IT THAT WAY), THE TIMING WAS EXCELLENT. THE DIRECTOR OF INTELLIGENCE FOR USEUCOM, MGEN H. P. SMITH, IS VERY INTERESTED IN SIGINT DECEPTION. RECENTLY HE SENT A MESSAGE TO [redacted] REQUESTING THAT THEY SEND A TEAM TO EUROPE TO BRIEF ON THIS SUBJECT (SEE REF ALFA). I SENT A COPY OF YOUR ARTICLE TO MGEN SMITH AND ON 24 MARCH HE WROTE THE FOLLOWING COMMENTS:

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

QUOTE

1. VERY INTERESTING! RIGHT ON!

2. IT SOUNDS LIKE THE AUTHOR IS NOT AWARE OF [redacted] --SO THOSE TWO ORGANIZATIONS SHOULD BE PUT IN TOUCH WITH ONE ANOTHER.

3. I WOULD SUGGEST ALL THE CRYPTOLOGIC ORGANIZATIONS GET TOGETHER FIRST AND POOL ALL THEIR KNOWLEDGE AND SPECIFIC EXAMPLES THEN ENLARGE A SUBSEQUENT MEETING TO INCLUDE GENERAL INTEL TYPES, PERSONS WITH ACTUAL EXPERIENCE IN COMBAT ZONES WHERE COMM DECEPTION HAS BEEN USED.

4. THEN CONDUCT COURSES IN EACH THEATER, PREPARE "TOOLS" AND "GUIDES."
END QUOTE

(CONFIDENTIAL - HVCCO)

ТРАНСЛИТЕРАЦИЯ ИЛИ КИРИЛЛИЦА?
TRANSLITERATsIYa ILI KIRILLITsA?
TRANSLITERATION OR CYRILLIC?
ТРЭНЗЛИТЕРЭЙШН ОР СИРИЛЛИК?

[redacted] P.L. 86-36

To be or not to be? That is the question. Whether 'tis nobler to transliterate or render in the original. . .

That's not quite how the quote goes, but the problem seems to have been around at least as long as Hamlet. I would also venture a guess that we here at NSA have collectively expended considerably more nervous energy on our problem than Hamlet did on his. It seems that every 3 to 5 years the spectre of transliteration raises its ugly head anew, and all the decisions we made in the last skirmish have to be "rediscovered" and "restated" yet another time.

Why this problem refuses to stay solved is difficult to determine. Could I suggest, however, that it is because we have not yet solved it?

Having spent about 10 years (1960-1969) transcribing, analyzing, and reporting Russian [redacted] I am aware -- painfully aware -- that discussions of transliteration tend to get very emotional and highly provincial.

In an attempt to lower the emotional content of this article, let me begin by offering a definition of transliteration and then explaining some concepts and properties of transliteration.

Transliteration, as I will be using the term, refers to transforming textual information from one alphabet to another. The properties of a good transliteration scheme are that the scheme should retain as much information about the original as possible, and that it should be easily learned and used by the persons using the particular scheme. In particular, I will be addressing only Russian-to-English transliteration. [redacted]

Editor's two-cents' worth

Before letting the author get into the body of his article, the editor feels that it might be advisable to take an explanatory side trip, to make certain that everyone knows exactly what transliteration *is* and what it *isn't*. Well, it isn't translation and it isn't transcription. Let's take the following hypothetical situation. You're Mike. You're on a tour of the Soviet Union. You'd like to meet some Russian girls, but your guide watches your busload like a hawk. Finally, one day, you and another guy (Joe) manage to exchange a few remarks with a cute-looking girl standing in line outside of Lenin's Mausoleum. You don't speak Russian, so Joe helps out. Here are a few of the interchanges.

Girl: **Дай мне поцелуй.**
Mike: What did she say?
Joe: **Дай мне поцелуй.**
Mike: No, I don't mean what did she *say?* I mean, what does it *mean?*
Joe: It means "Gimme a kiss!"

Girl: **Как тебя зовут?**
Joe: She wants to know your name.

Girl: **Меня зовут Тамара.**
Joe: She says her name is Tamara.

Girl: **Как вам нравится Москва?**
Joe: She wants to know how we like Moscow.

Just then the guide shows up and shoos you both back onto the bus. [redacted] EO 1.4.(c) P.L. 86-36

Mike: See you "Tamara"! -- same time, same place!

On the bus, you write down in your handy-phrases notebook (for a nonlinguist, you have excellent auditory acuity and retentivity):

Diamon' yeah putza Louie.
Kahk tibyah zuhvoot?
Minyah zuhvoot Tamara.
Kakh vahm nraveetsa Muskva?

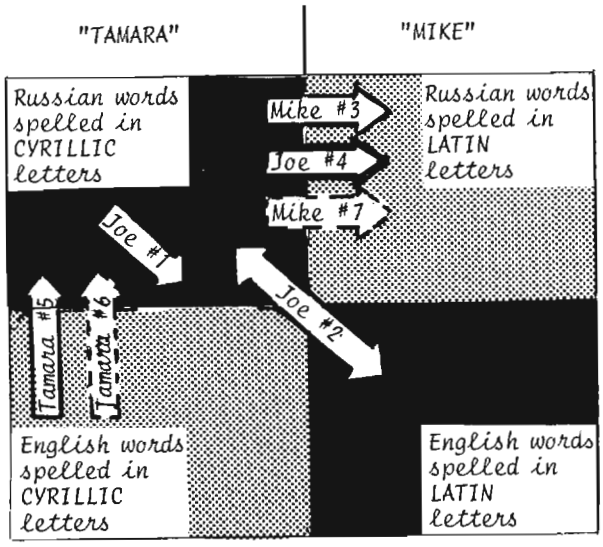
Joe looks over your shoulder and says, "You're spelling everything all wrong!" He crosses out what you wrote and puts down:

Day mne potseluy.
Kak tebya zovut?
Menya zovut Tamara.
Kak vam nravitsya Moskva?

Meanwhile, back at the Mausoleum, Tamara has jotted down two names in *her* notebook:

Майк, Джо

A lot happened during these brief interchanges, linguistically (if not romantically) speaking. Let's extrapolate everything into a representation of the entire Russian language (left-hand side, "Tamara") and the entire English language (right-hand side, "Mike").



When Mike asked, "What did she say?" and Joe answered, "She said, **Дай мне поцелуй**" (arrow "Joe #1"), that didn't help Mike much. It was still in Russian! When this process occurs in the COMINT business (that is, listening to people talking in Russian, then putting down on paper, *in Russian*, what they said) it is called TRANSCRIPTION. The process is concerned, sure enough, with what the speaker *said* (his exact words, as he spoke them), but it doesn't help the nonlinguist analyst any. He still doesn't know what it means! (Incidentally, even though this step doesn't yield the English meaning, the voice transcriber has a hard job to do, and he certainly has to *know* what the person is talking about before he can transcribe it.)

What Joe did, after his first little "joke," was to INTERPRET for Mike and Tamara (arrow "Joe #2"). Interpretation is translation, usually back and forth, from one *spoken* language to another. People in the COMINT business rarely are involved in interpretation. Instead, they are usually involved in TRANSLATION (the transformation of text in one *written* language to another written language -- and usually NSA translators specialize in the "into English" direction). Interpretation and translation are concerned with what the utterance *means*. Mike and the NSA nonlinguist don't care a rat's whisker about how the linguist derives the meaning, or how hard it is to master those complicated morphologic and syntactic rules. For example, Joe didn't bother to tell Mike that he changed Tamara's "How does Moscow please itself to you?" to "How do you like Moscow?" or to explain that he "translated" the name of the Russian city from "Moskva" to English "Moscow." As far as the nonlinguist is concerned, it's as easy for the translator to translate as it is for the transcriber to transcribe. So the nonlinguist feels that that should be the end of the problem.

What, then, are those other five arrows doing in the chart? They do not deal with the meanings of the words, but only with their representation in printed form.

When Mike decided, for example, to record the Russian sentences he wanted to remember (arrow "Mike #3"), he did something similar to TRANSCRIPTION ("Joe #1"). But, instead of COMINT-style transcription (writing down on paper the utterance in the original language, as spelled in the original alphabet), he tried to record the Russian sentences in Latin letters on the basis of the Russian *pronunciation*. (This can be done scientifically, but when it's done by amateurs like Mike, it usually looks weird.)

When Joe looked over Mike's shoulder and "corrected" the spelling (arrow "Joe #4"), he was -- we're finally hitting paydirt! -- engaged in TRANSLITERATION. This is what this article, once we get to it, is all about: the spelling of Russian words in Latin letters on the basis of their original Cyrillic *spelling*. The problem is, "Who's got the one true system?" Joe used a system of transliteration in which the Russian letter **й** is represented by "y." If he had used the NSA system, he would have written, *"Daj mne potseluj!"* (non-NSAers say that all those "j's" "look funny").

When Tamara wrote the two names in her notebook (arrow "Tamara #5"), she TRANSCRIBED the names into Cyrillic on the basis of their *sound*. She wrote **Майк** and **Джо**. She would have been wrong (arrow "Tamara #6") to transliterate them according to their *Latin spelling*: **Мике** and **Йое** (that would make them pronounceable in Russian as "Meek-yeah" and "Yoh-yeah"). Ridiculous, isn't it? And yet there are English words in the Russian language which are spelled in Cyrillic and pronounced in Russian in such a ridiculous way.

If Mike were ever to read Tamara's notebook and laboriously transliterate the two names into Latin characters (arrow "Mike #7"), he would obtain "Mayk" ("Majk") and "Dzho." Would he recognize his own name or Joe's? Or would

he be completely unaware that he had come up against one of the translator's biggest problems -- the rendition of non-Russian personal names, place names, etc. not by transliteration but by restoring them to their original Latin spellings: not "Nikson," "*Taym* magazine," "Reno," but "Nixon," "TIME magazine," and "Renault."

Transliteration as we will discuss it, then, is a very specific operation: the transformation of Russian text, in Cyrillic characters, into the Latin alphabet according to a specific preferred scheme. The transliteration process does not produce a translation, but carries into the Latin representation all the grammatical information present in the Cyrillic text. Hence the meaning content of the Latin-transliteration text is identical with the meaning content of the original Cyrillic text, and both texts would yield the identical translation.

Several Russian-to-Latin transliteration schemes have been developed. Table 1 shows only a few of them. The list of schemes is not intended to be exhaustive, but, rather, to show the "flavor" of the transliteration world. The various schemes conform, to a greater or lesser degree, to the requirements of accuracy (that is, nonambiguity) and ease of use. Of particular interest is the various handling of the Cyrillic letters

Ъ, ъ, ж, й, х, ц, ч, ш, щ, ъ, ь, э, ю, я

(14 out of the 33 letters in the Russian alphabet).

Note that:

- [redacted] most schemes use combinations of Latin characters to represent certain Cyrillic characters (that is, the Cyrillic and Latin characters do not constitute a one-to-one mapping);
- [redacted] most schemes contain inherent ambiguities, in that certain combinations of Latin letters can represent two different Cyrillic situations, and it is sometimes impossible to tell from context which of the two possible Cyrillic situations had occurred in the original text. (For any mathematicians still reading, they are not an "onto" mapping).

The question which should arise at this point is, "Why?" Why transliterate? Or, if you must, then why in so many different ways? Or even, why worry about the fact that Joe likes [redacted] while Tom likes [redacted] and Harry simply has to have BGN?

The answer to the simplest of these questions is clear, and is probably a derivative or corollary to Murphy's Law: "If Tom, Joe, and Harry,

Table 1

Russian	*Board on Geographic Names*	*Library of Congress*[1]	*International Standards Orgn.*
А	A	A	A
Б	B	B	B
В	V	V	V
Г	G	G	G
Д	D	D	D
Е	E, YE[2]	E	E
Ё	E, YE[2]	E	Ë
Ж	ZH	ZH	Ž
З	Z	Z	Z
И	I	I	I
Й	Y	I	J
К	K	K	K
Л	L	L	L
М	M	M	M
Н	N	N	N
О	O	O	O
П	P	P	P
Р	R	R	R
С	S	S	S
Т	T	T	T
У	U	U	U
Ф	F	F	F
Х	KH	KH	H
Ц	TS	TS	C
Ч	CH	CH	Č
Ш	SH	SH	Š
Щ	SHCH	SHCH	ŠČ
Ъ	"	"	"
Ы	Y	Y	Y
Ь	'	'	'
Э	E	E	È
Ю	YU	IU	JU
Я	YA	IA	JA

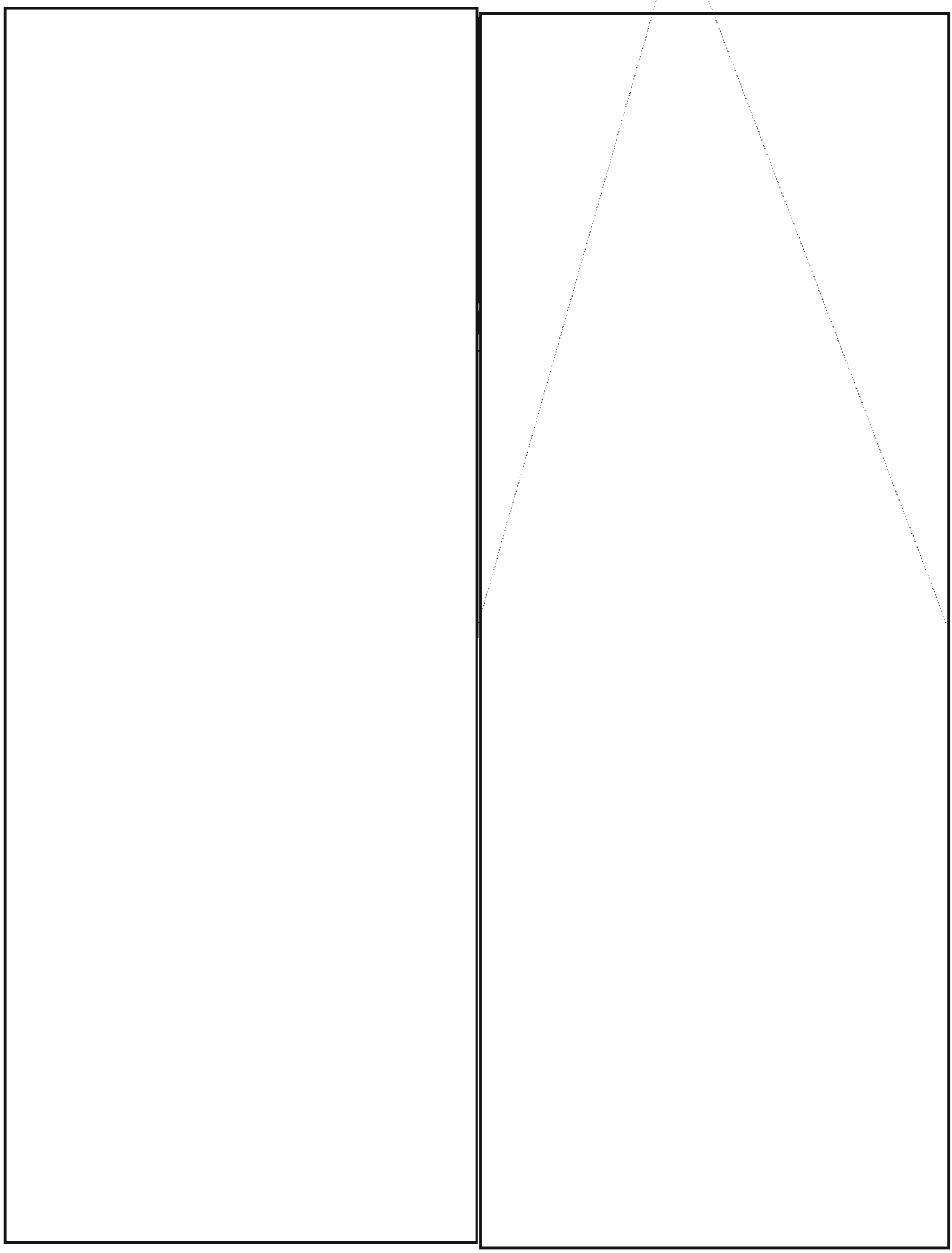
[1]"Modified" system, which omits the diacritics used in the preferred LC system.

[2]E or Ë when preceded by consonant. Otherwise (initial, or when preceded by vowel) YE or YË.

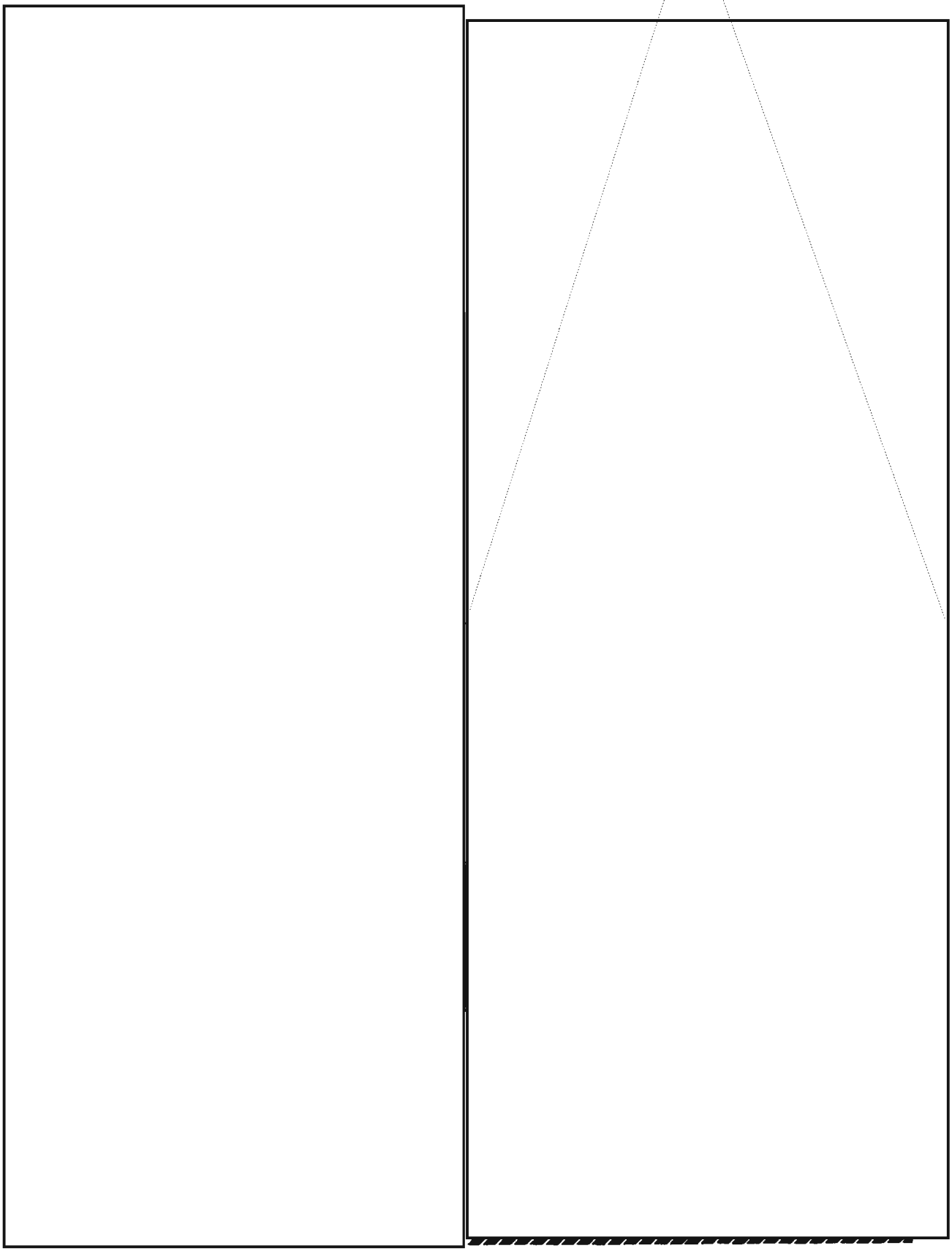
as noted above, keep their data in different transliteration schemes, then they *shall* be tasked to produce a joint report, or else, because of their own respective missions, they *shall* find it absolutely necessary to merge two (or more) of the computer data files involved here."

[redacted]

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



~~CONFIDENTIAL~~



COMMENTS AS REQUESTED! (More on the AG-22/IATS)

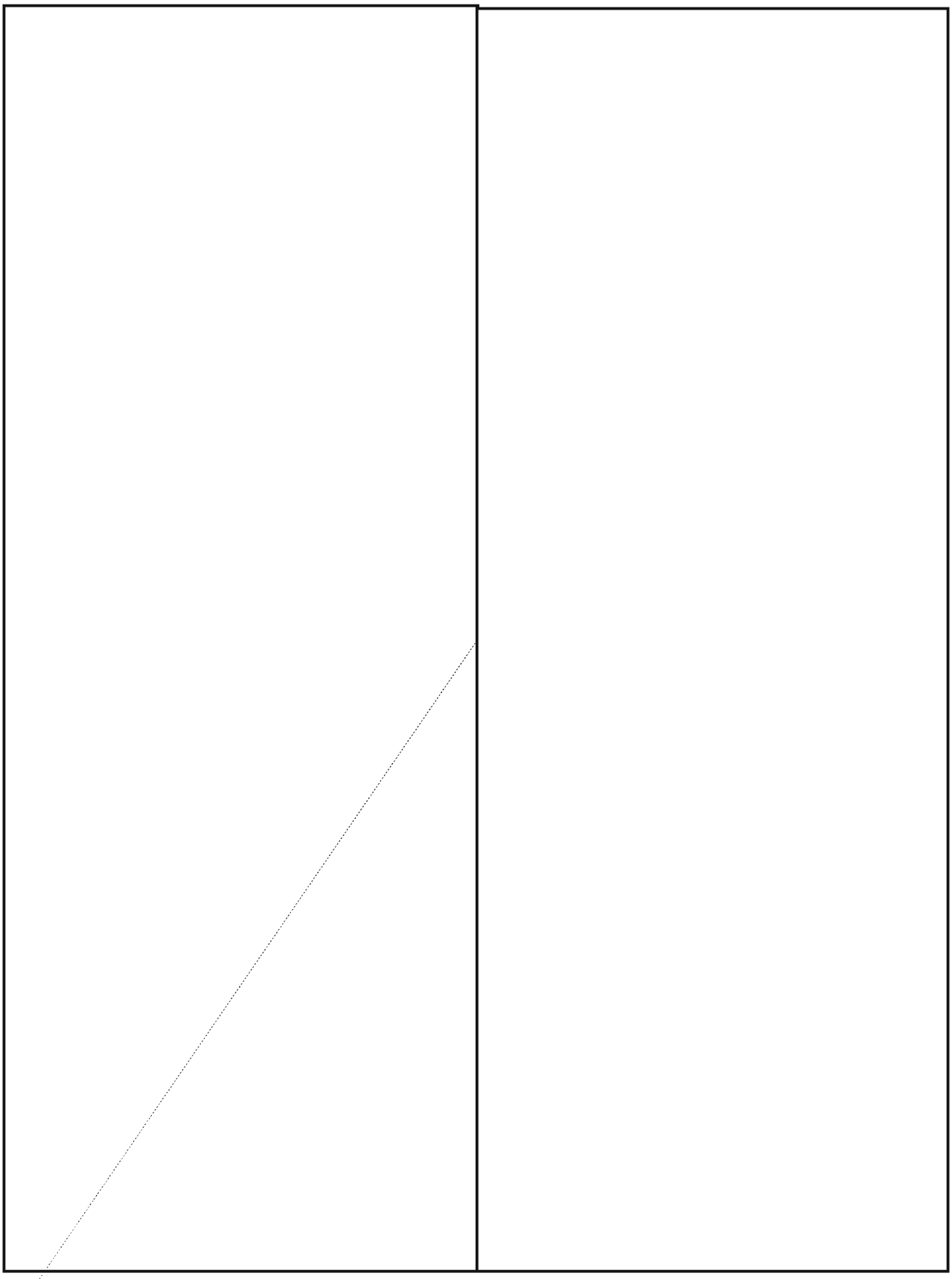
P.L. 86-36

At the end of his article, "Musings About the AG-22/IATS" (CRYPTOLOG, March 1976), Cecil Phillips asked, "Comments, anyone?" Well, comments he's received! [redacted] ("What's Wrong With AG-22/IATS?") appeared in the May 1976 issue of CRYPTOLOG. The following comments which were recently received seem to be worth publishing in full, despite their slight overlappings in treatment. CRYPTOLOG would continue to welcome further comments of a substantive nature on this subject.

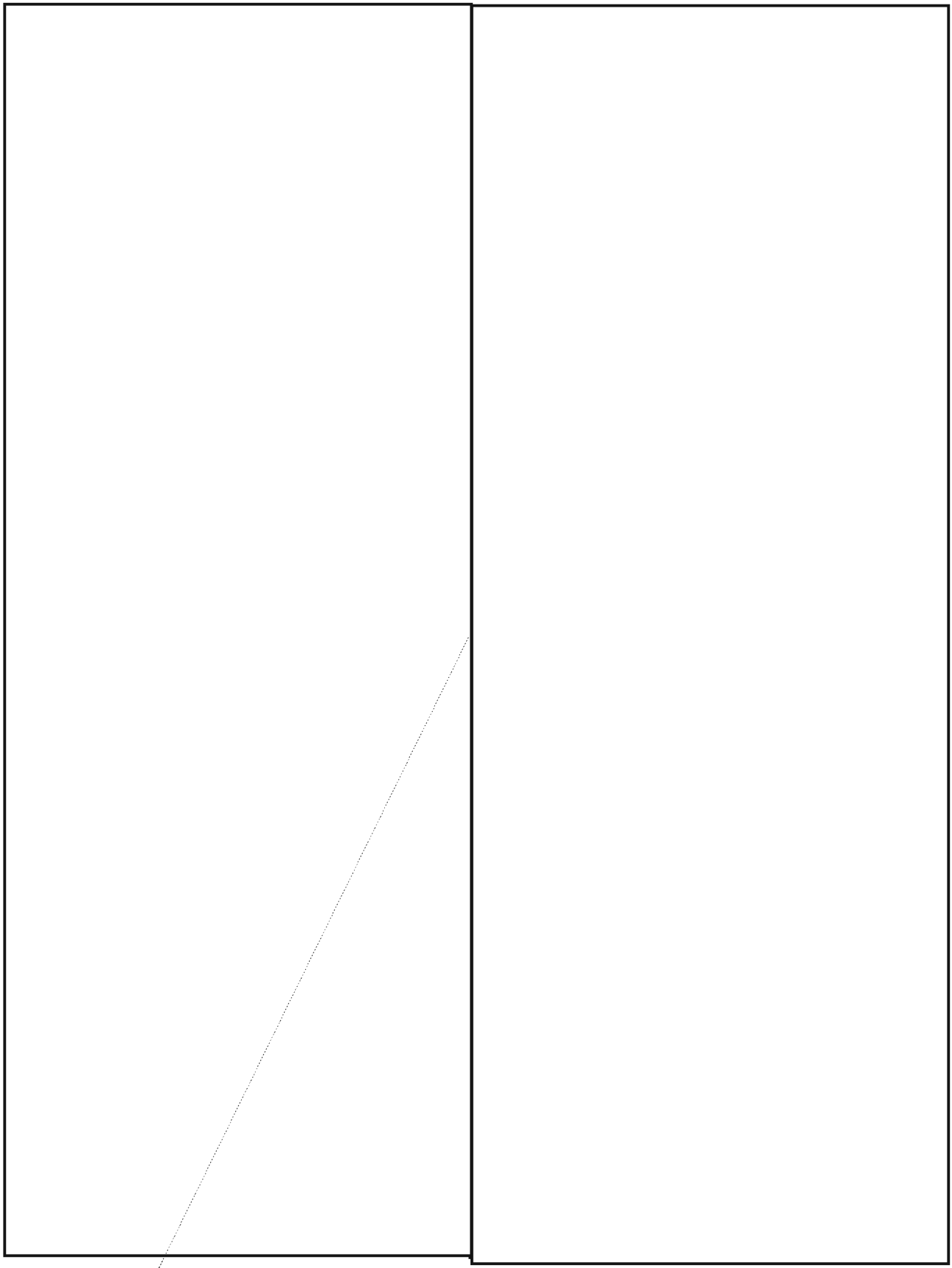
Ed.

[redacted]

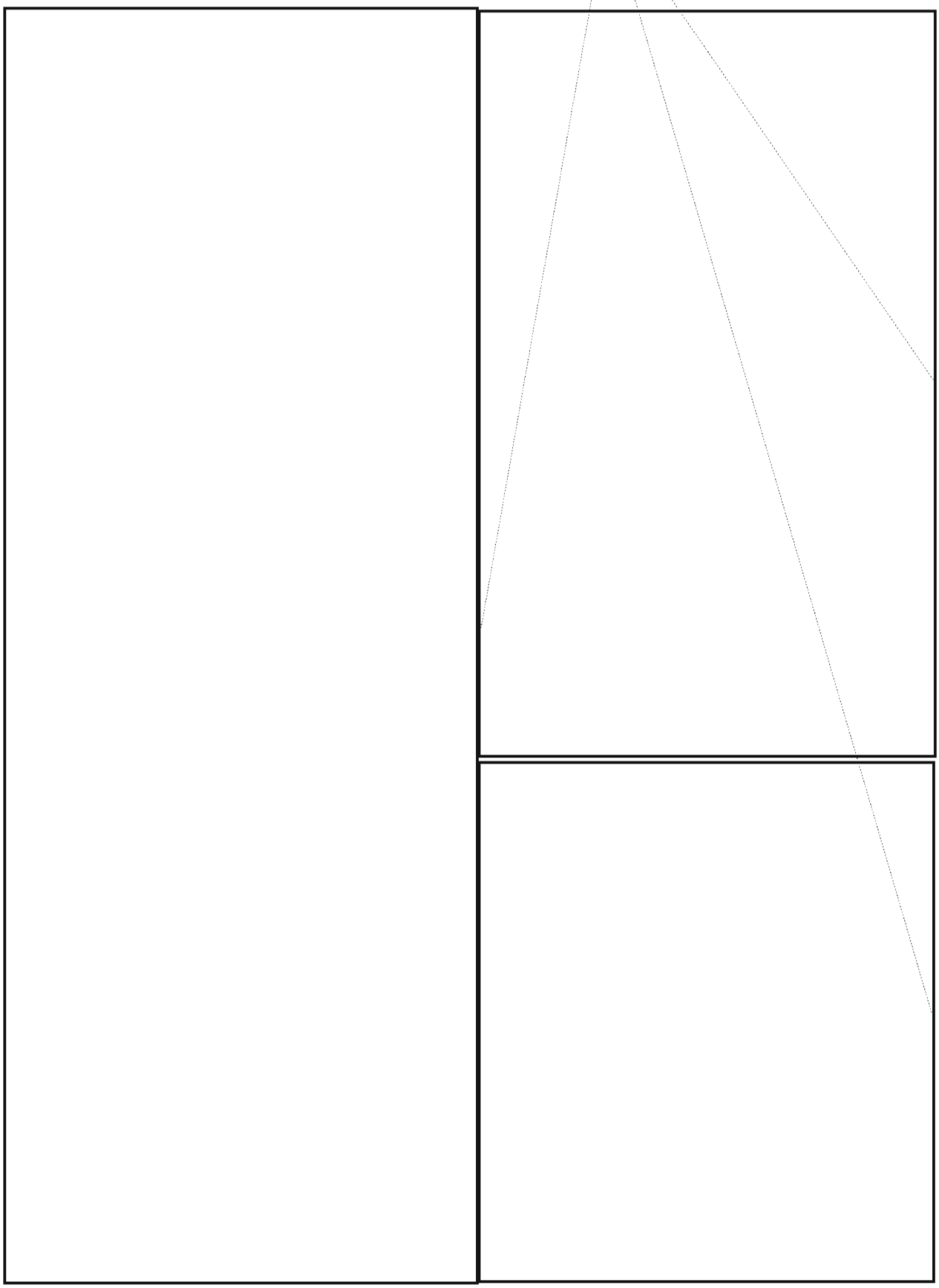
[redacted]

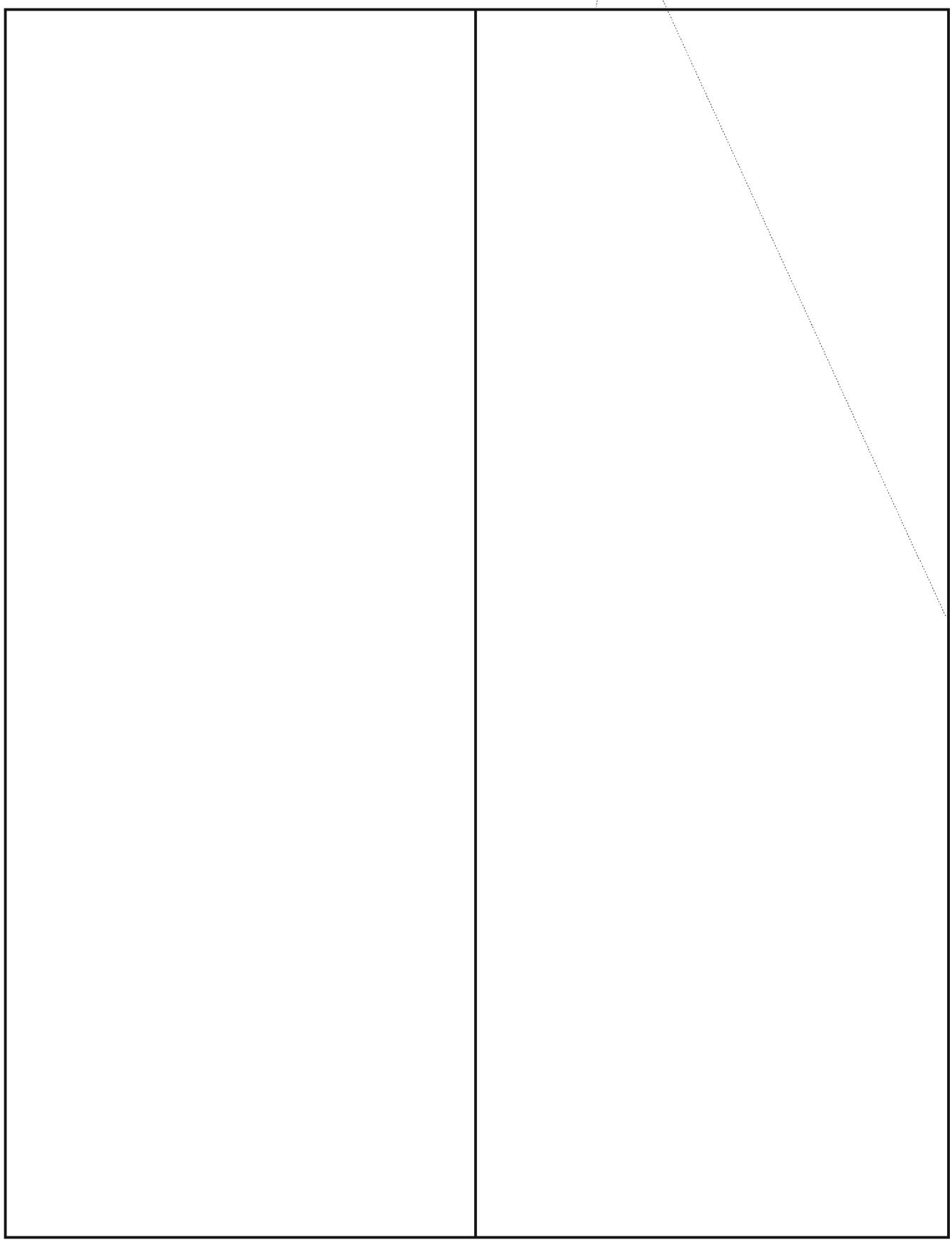


P.L. 86-36
EO 1.4.(c)



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





NSA-CROSTIC NO. 4

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

A. Allegedly the ones most likely to appreciate SST flights (2 wds)

B. Abnormally enlarged masses of lymphoid tissue at back of the pharynx

C. Pseudonym of Emmanuel Poiré, French caricaturist (2 wds; read as one word, a Russian pun)

D. "--- man out" (game)

E. Covered stone bridge in Venice, connecting ducal palace with the state prison (3 wds)

F. What circling tigers in *Little Black Sambo* turned into

G. Ignored

H. French painter of flowers (famous for paintings of roses) (1759-1840)

I. "Sleeping Woman," dormant volcano in Mexico (last eruption, 1868)

J. State (abbrv)

K. He "opened up" Japan (2 wds)

L. Poem by Rudyard Kipling

M. Scout

N. Hot mixed drink, topped with whipped cream (2 wds)

O. Popular U.S. dance for several decades prior to 1910; superseded by fox trot

P. Despite what NSA linguist's father (Georgia, late 1940's) said when son decided to major in Spanish ("If English was good enough for Jesus, it ought to be good enough for you!"), the language spoken by Jesus

Q. Sharpen again

R. Japanese admiral; at time of Pearl Harbor attack, commander-in-chief of combined fleet

S. What showoff Fritz said to his brother (they had been mountain-climbing with their mother) (4 wds)

T. One of the mightiest rivers of the Indian subcontinent

U. Partially compacted granular snow that forms the surface part of the upper end of a glacier

WORDS

A.	20	180	55	120	35	73							
B.	23	50	67	5	88	31	164	34					
C.	62	42	97	103	80	57	37	107	125	27			
D.	95	170	174										
E.	87	167	143	130	6	182	112	18	10	45	71	162	61
F.	16	117	157	175									
G.	178	92	78	131	53	158	118	144					
H.	66	163	1	29	96	51	140						
I.	173	176	7	19	155	74	63	2	39	83	104		
J.	46	150											
K.	141	21	124	100	72	25	13	114	79	41	85	76	
L.	14	110											
M.	105	91	12	152	109	33	90						
N.	70	132	43	149	8	177	17	82	99	58	64		
O.	40	145	159	171	60	93	22						
P.	142	3	106	181	168	49	111						
Q.	115	65	139	101	15	126							
R.	127	172	28	81	113	98	138	135					
S.	75	136	166	108	11	86	119	38	24	122	69	48	
T.	4	59	68	128	26								
U.	153	147	30	116									

V. Where agreement that ended the War of 1812 was signed — 47 94 151 148 102

W. Not discarded — 56 129 179 146 9 137

X. Influence — 121 160

Y. Highest peak in Wales — 133 44 154 77 36 165 123

Z. Swiss tourist resort and munitions town (something for everyone!) — 161 52 89 169

Z_1. Shooting at clay targets — 54 156 84 32 134

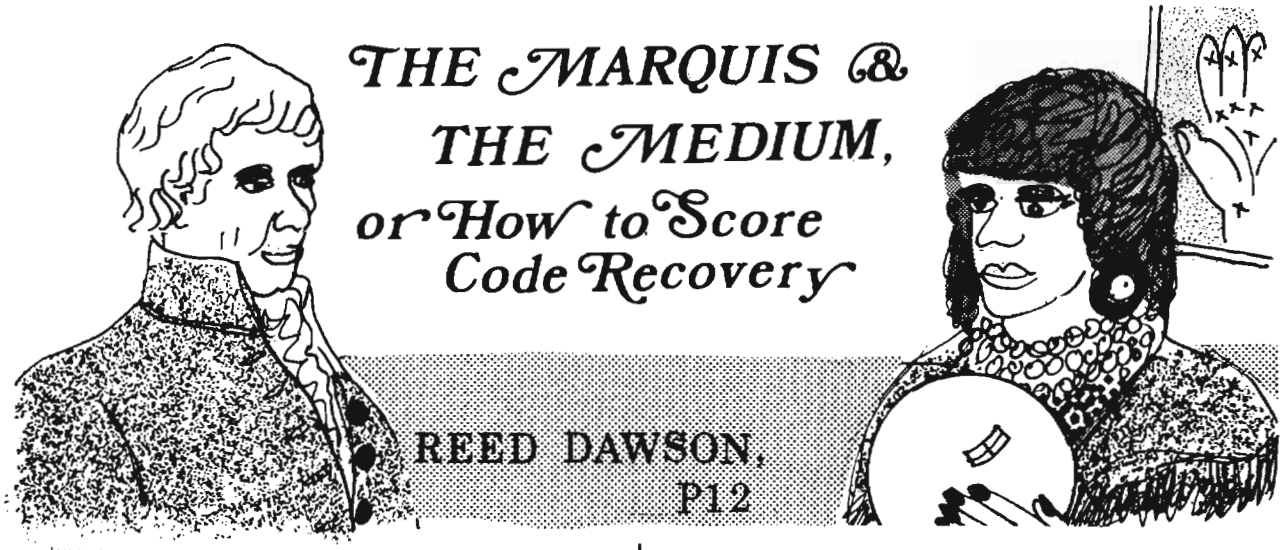
1 H	2 I	3 P	4 T	5 B	6 E		7 I	8 N	9 W		10 E	11 S	12 M	13 K	14 L
15 Q	16 F		17 N	18 E		19 I		20 A	21 K	22 O	23 B	24 S	25 K	26 T	27 C
	28 R	29 H	30 U	31 B	32 Z_1		33 M	34 B	35 A	36 Y		37 C	38 S		39 I
	40 O	41 K	42 C	43 N	44 Y	45 E	46 J	47 V		48 S	49 P	50 B		51 H	52 Z
53 G		54 Z_1	55 A	56 W	57 C	58 N	59 T	60 O	61 E		62 C	63 I	64 N	65 Q	66 H
67 B	68 T		69 S	70 N	71 E	72 K	73 A	74 I	75 S	76 K		77 Y	78 G	79 K	80 C
	81 R	82 N	83 I	84 Z_1	85 K		86 S	87 E	88 B	89 Z	90 M		91 M	92 G	93 O
	94 V	95 D	96 H	97 C		98 R	99 N		100 K	101 Q	102 V	103 C	104 I		105 M
106 P	107 C	108 S		109 M	110 L		111 P	112 E	113 R	114 K	115 Q	116 U	117 F	118 G	119 S
120 A	121 X	122 S	123 Y		124 K	125 C	126 Q	127 R		128 T	129 W	130 E	131 G	132 N	133 Y
134 Z_1	135 R	136 S	137 W		138 R	139 Q	140 H		141 K	142 P	143 E	144 G		145 O	146 W
147 U	148 V		149 N	150 J	151 V		152 M	153 U	154 Y	155 I	156 Z_1	157 F	158 G		159 O
160 X		161 Z	162 E	163 H		164 B	165 Y	166 S	167 E		168 P	169 Z	170 D		171 O
172 R	173 I	174 D		175 F	176 I	177 N	178 G	179 W	180 A		181 P	182 E			A.J.S.

(Solution next month.)

CMI BANQUET, at GODDARD SPACE FLIGHT CENTER, Friday, 18 JUNE 1976, 6:30 p.m.

Open bar -- prime rib dinner --NASA tour.

TICKETS: $8.50 (CMI member; one guest of CMI member); $10.00 (all others).
Reservations: Rose Campbell, P1, 3W090, x3957s.



THE MARQUIS & THE MEDIUM, or How to Score Code Recovery

REED DAWSON, P12

"Mais, monsieur," Madame Claire was saying, "never have I been asked to dig so deep."

The placards in the second-floor window had caught my eye. Spirit communications vied with palmistry, astrology, tea-leaf readings, and Egyptian sand divinations. But for the "on parle français," I'd not have entered, tendering an ephemeral greenback.

I wanted to question Pierre-Simon de Laplace (1749-1827), the famous French mathematician and astronomer, about his notorious law of succession. The law says that if an event has occurred k times in n trials at some fixed but unknown probability, then the odds for the next trial are to be estimated as $k+1$ to $n-k+1$ in favor of occurrence. Laplace had gone so far as to apply the law to the odds the sun would rise the morrow morn, for which he had often been upbraided in limbo.

"Try," I urged. And lo, after an agony of mutterings and eye rollings, Madame Claire claimed to have the spirit of the Marquis de Laplace. As a test, I inquired politely about the rising sun. It was a mistake. An angry French voice issuing from the medium shot back, "Imbécile, if you wish to consider collateral information, then do so!"

I rallied, firing the twenty-dollar question. "Your law of succession doesn't seem to apply to many-celled multinomial distributions, the kind where the number of cells is more than the sample size. When one forms odds by adding unity to each cell count, the odds on the unseen categories become impossibly large."

"Mon enfant," he replied, more in pity than anger, "naturellement one must count the live cells only. Can you not estimate their number?"

The medium woke with a gasp. "C'est tout, monsieur. Au revoir."

"Mais c'est merveilleux! Please, one more and we will both become famous."

"What is it that I must do?" She regarded my emerging wallet with suspicion.

"Just one more Pierre-Simon, madame, I beg you. Pierre-Simon de Fermat, for just one little question."

"And when did this one die, monsieur?"

"In 1665."

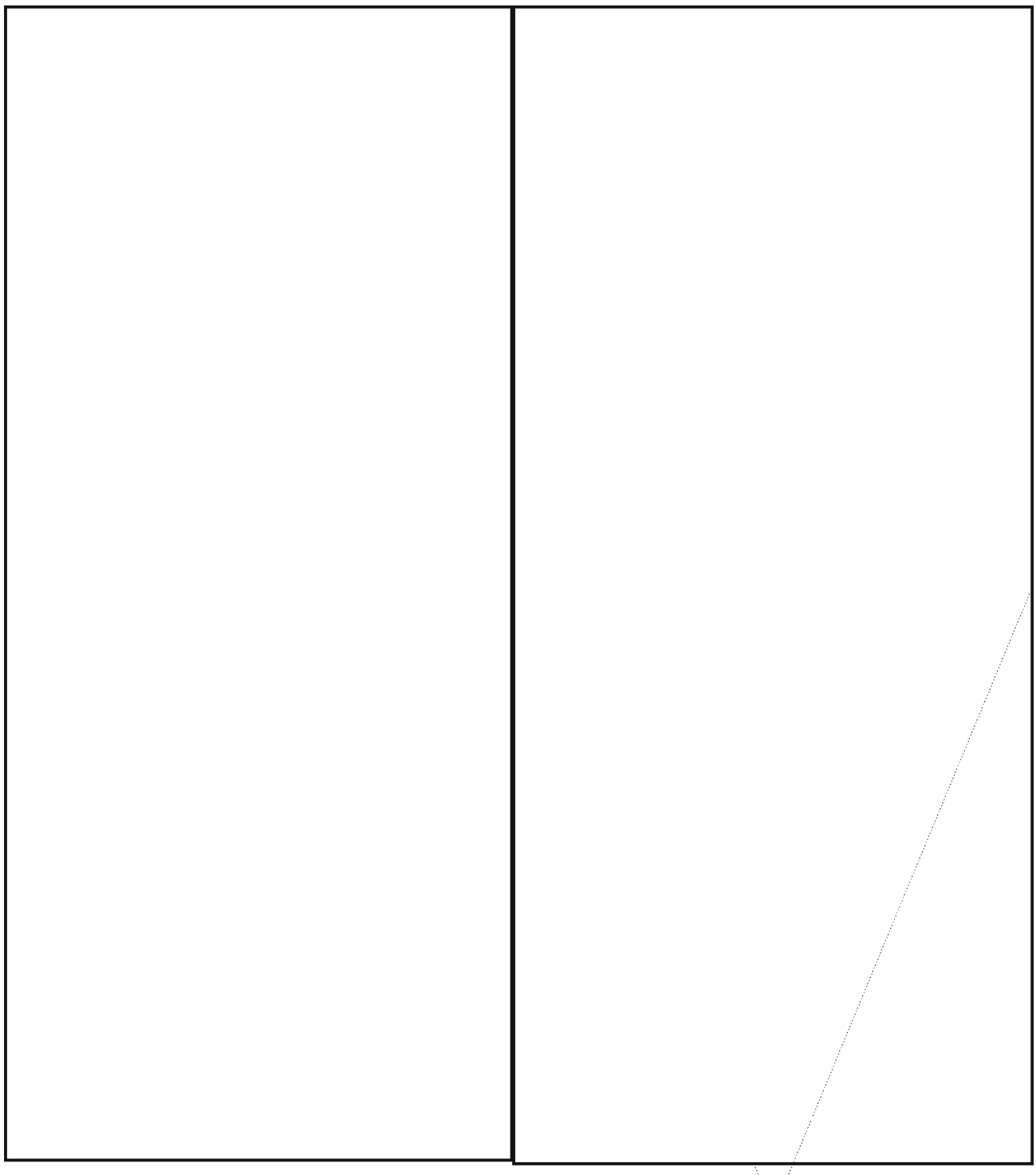
"Mon Dieu, monsieur! Adieu, monsieur."

For further details, see "A Survey of Multinomial Estimation for Code Weighting," *NSA Technical Journal*, Vol. 20, No. 3, Summer 1975.

~~(CONFIDENTIAL)~~

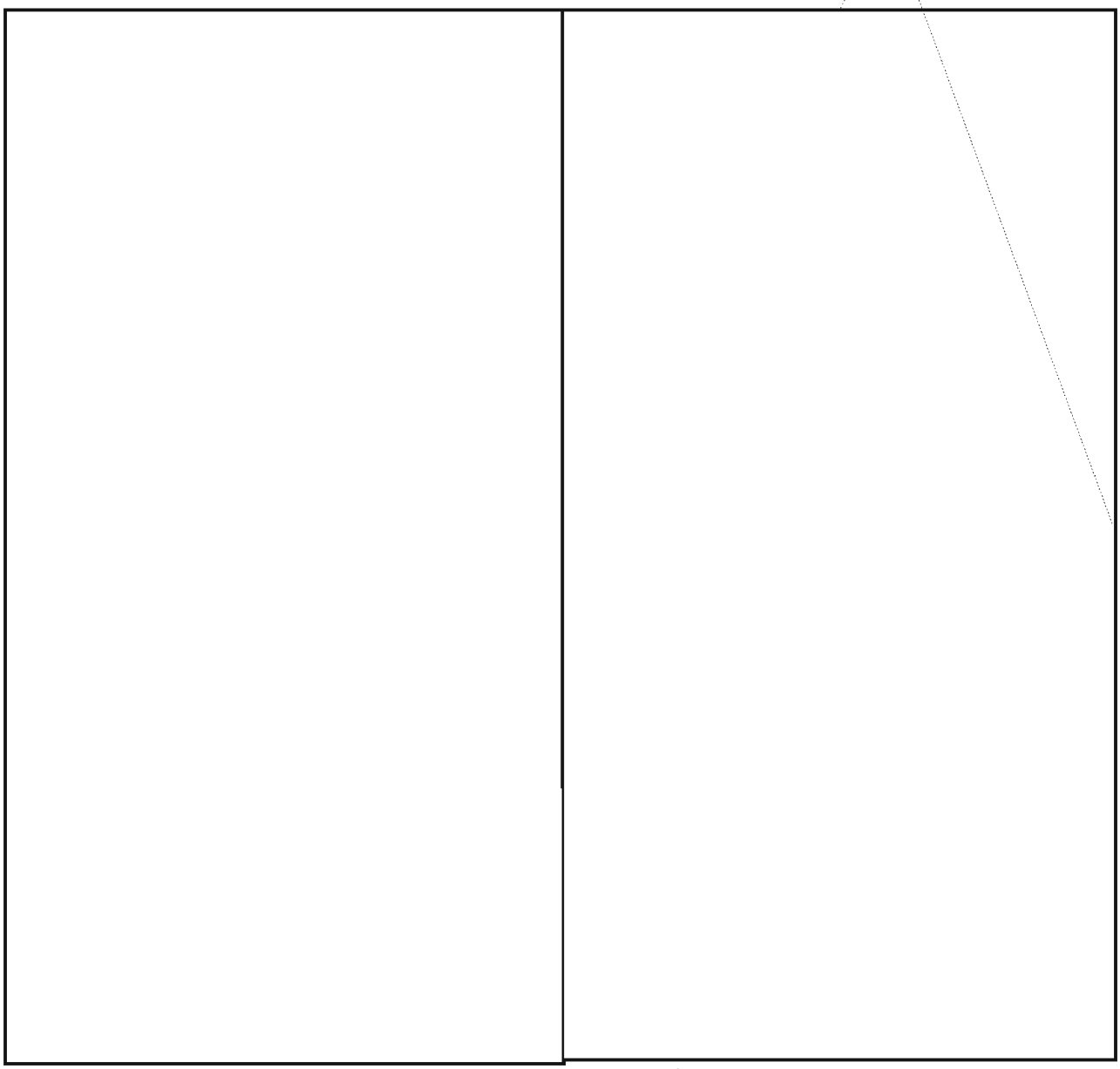
THE [redacted] COLLECTION SYSTEM

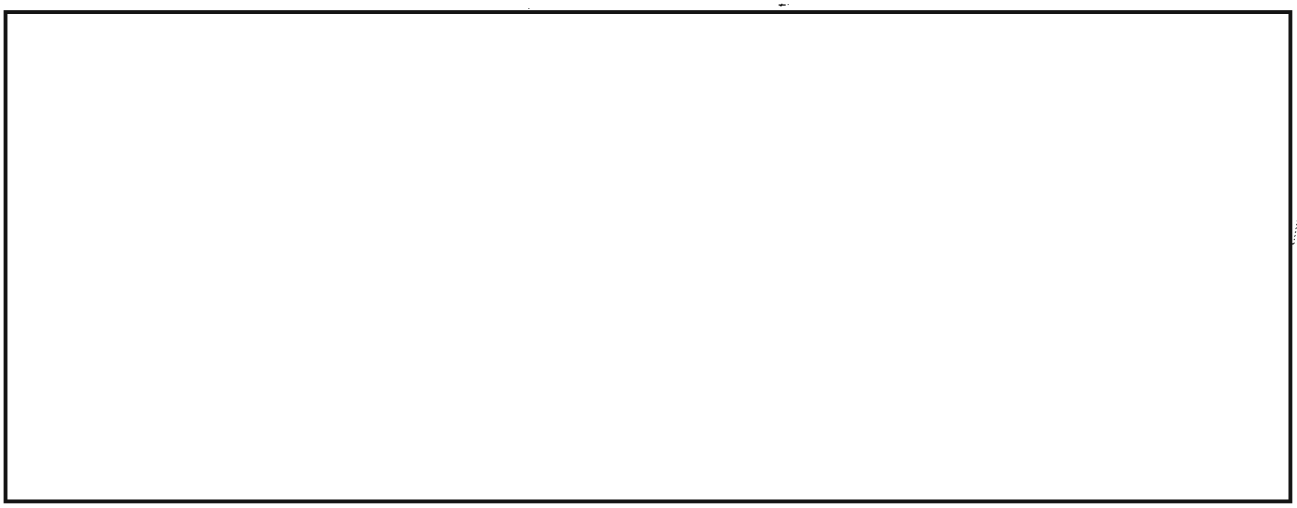
Tim Murphy, B341



~~SECRET SPOKE~~

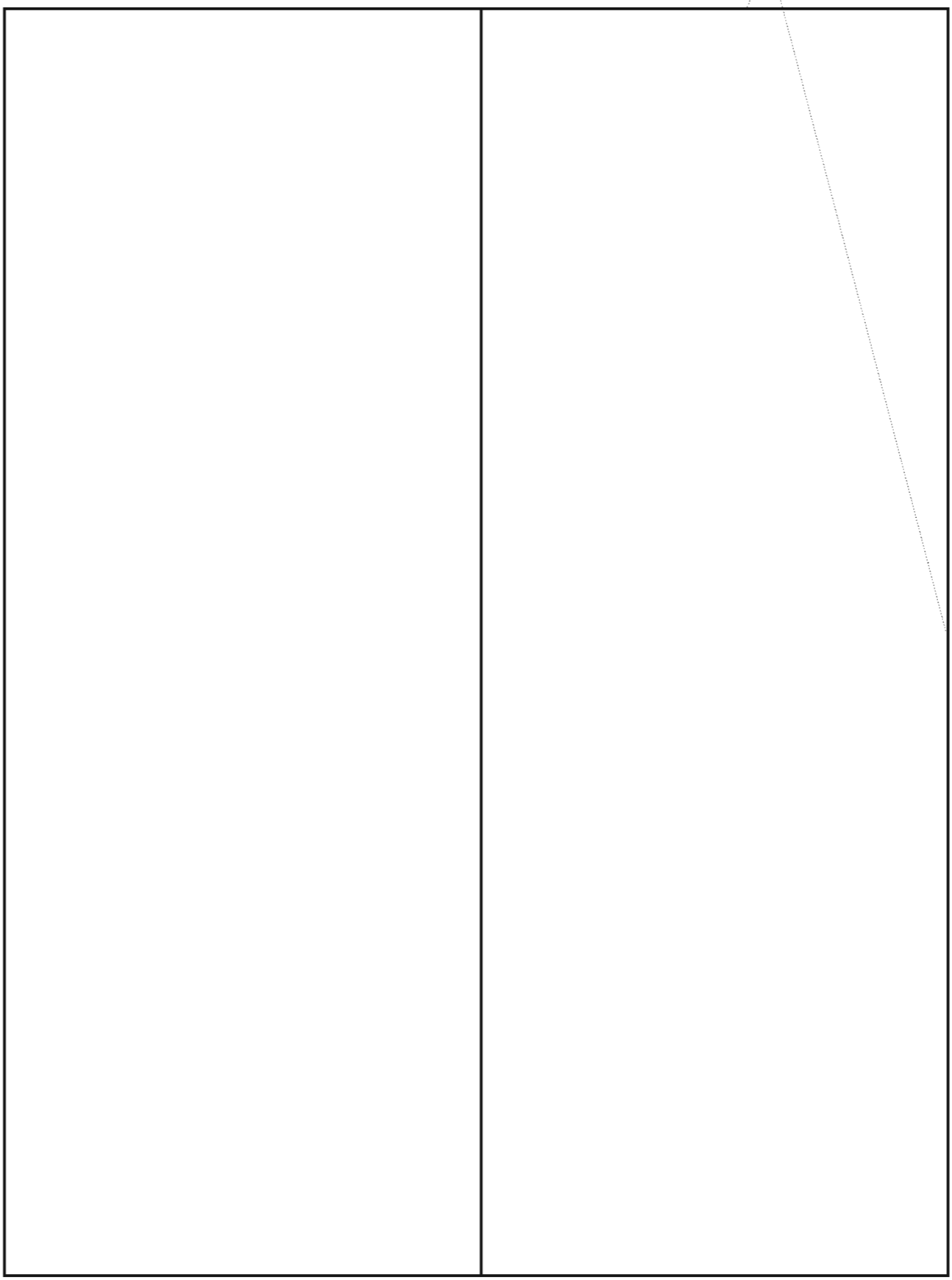
EO 1.4.(c)
P.L. 86-36





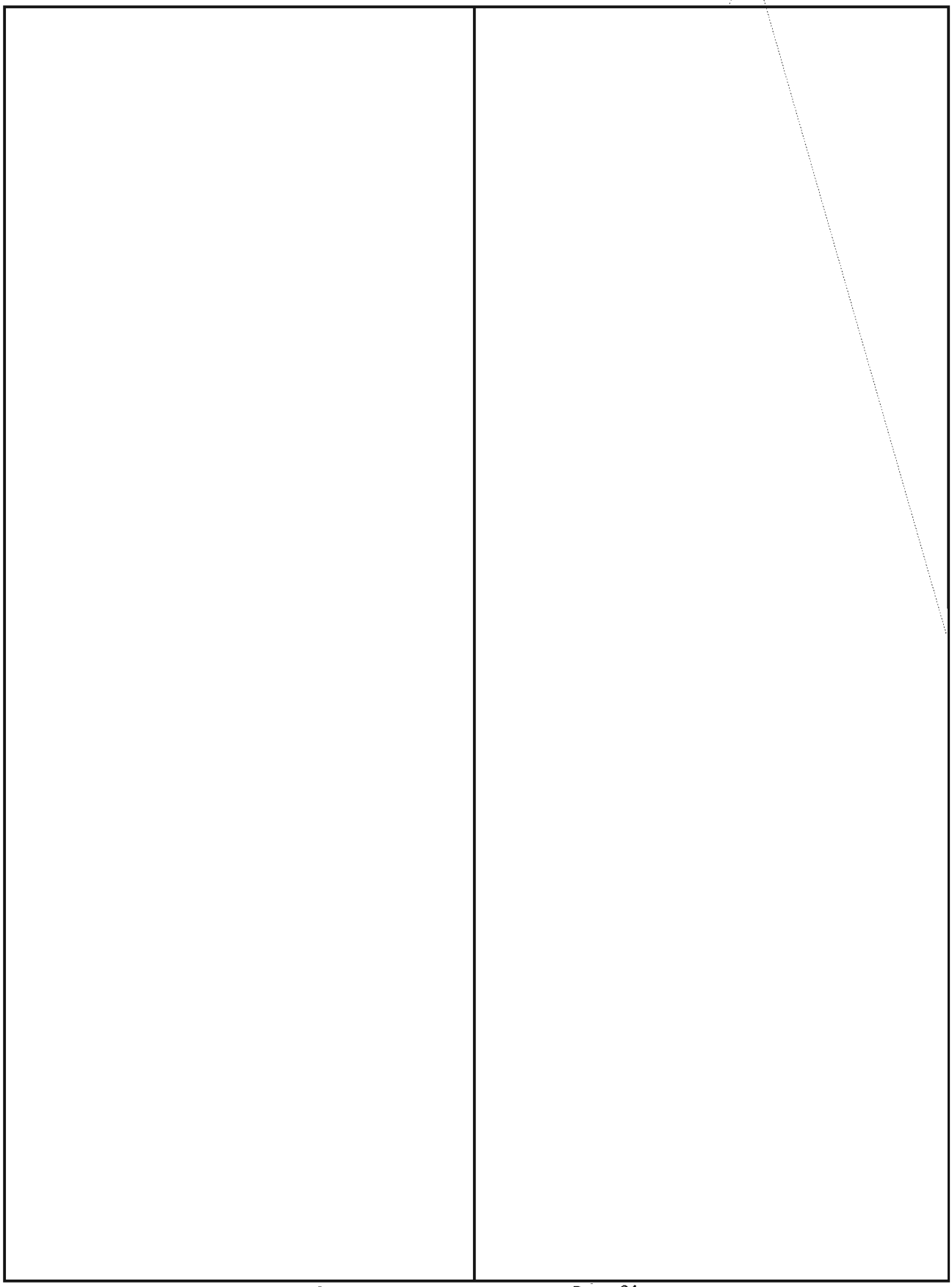
EO 1.4.(c)
P.L. 86-36

~~SECRET SPOKE~~



~~SECRET SPOKE~~

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



[redacted]

~~(SECRET SPOKE)~~

Comments as requested

(*Continued from page 17*)

[redacted]

~~(CONFIDENTIAL HVCCO)~~

HOW THINGS HAVE CHANGED!

[redacted] H111 P.L. 86-36

"Bei dir ist es nun soweit, Baby!"

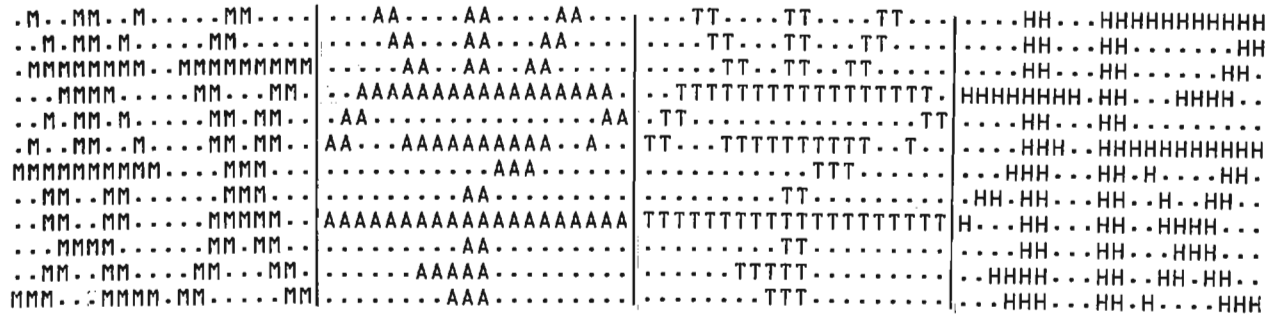
As a member of the Cryptanalysis Career Panel, I am interested in the selection and development of people with the best potential for becoming professional cryptanalysts. In doing research in this field recently, to trace the historical trends in cryptanalyst recruitment at the Agency, I came across a description of one approach that had been taken by a competing agency not too long ago.

The description occurred in the second part of the two-part article "On the Selection of Cryptanalysts," by Alex Dettmann (*NSA Technical Journal*, Vol. V, No. 1, January 1960, and No. 2, April 1960). The author is identified as follows: "The author of this paper was a former lieutenant in the German Army. As officer-in-charge of the Russian Section of the Cipher Bureau of the German Army High Command, he gave considerable thought to the selection and training of professional cryptanalytic personnel." The paper, which dealt with the historical development in the years 1935-1945, was written from memory after World War II.

Says Dettman:

> Even with the danger of being considered old-fashioned and unobjective, the author rejects the assignment of female personnel categorically and without exception as cryptanalysts though not as clerks or assistants. Quite apart from the fact that the subject matter as such is foreign to a woman's mentality, it must be added that it is extremely difficult for most women to engage in work about which no word may be spoken. During his long years in a managerial status, with the opportunity of becoming acquainted with most of the cryptanalytic positions in the former German Republic, the author has never known a single woman who did even average work as a cryptanalyst. All of the women who were assigned during and after 1943 as staff or intelligence assistants (a bare total of about 100) can only be described as clerical personnel or more or less efficient assistants.

~~(CONFIDENTIAL)~~



CHINESE MT (MACHINE TRANSLATION)

Like the two-way radio wristwatch, machine translation (MT) of language continues to fascinate certain segments of the scientific-technical and intelligence communities. As interest in Russian-to-English MT lessens, we observe a new area of interest -- Chinese-to-English. The following two articles, which deal with the same Chinese-to-English MT project, arrived at the editorial office in the same week. With Agency interest like this, the editor feels compelled to print both articles in their entirety, despite the slight overlapping of the authors' comments.

Ed.

NOTES ON TRANSLATION FROM THE CHINESE

[redacted] R51

P.L. 86-36

The Department of Computer Science of the United College of the Chinese University of Hong Kong has its own machine-translation project. First announced offspring of the project is the CULT (Chinese University Language Translator) System, which is being used, we understand, to translate, inter alia, *Acta Mathematica Sinica*. In July 1975 we saw their translations of all six articles in the September 1974 issue. We did not, then or later, see the original articles in their pristine ideographic form.

In January 1976 we found ourselves in (licit) possession of a nine-page package centered about a one-page article from the journal cited earlier.

A word (perhaps two) about the contents of those nine pages. Page 1 was, of course, the original article, characters and all (and the characters in some cases were what the Chinese themselves call "simplified" -- in any case they're different from their "traditional" predecessors). The next two pages contained the translation into English by some anonymous Chinese mathematician. Following these were the two pages of "input" to the CULT System.

At least two more words are necessary here: the computer never got to "see" the ideographs. In their place it saw the appropriate four-digit values from the well-known Standard Telegraphic Code (STC). Since the new, "simplified" characters have not made their appearance in STC, each one in the original journal article was replaced by the "traditional" one.

The computer never got to translate the title of the article: the human's translation was entered, in English, along with the rest of the input.

All "equations" were copied (presumably photocopied) without any computer translation

being allowed to intervene. Thus, for example, the character meaning "or" was replaced in one equation by "or," although that same character (in STC guise) occurred in the textual portion of the article (and was indeed translated as "or").

Back to the table of contents.

The next two pages were the (mildly edited) Chinese original -- edited in the sense that the simplified characters have been replaced by their ancestors, and certain shortcomings of the CULT System have been compensated, in advance, by the project workers. As a tiny example, the article begins by stating that certain alphabetic symbols (our alphabet and also that of the Greeks) stand for real numbers. The Chinese are content to say "a, b, c real numbers." But in the edited input, the simple string "a, b, c" was changed to "a, b *and* c."

Finally, the last two pages contain the computer's translation of the mildly edited, amplified, historically adjusted, original article.

In my opinion, both translations -- its and his (maybe hers, but could the Chinese be that civilized?) -- were pretty good. The fact that both translations, in their own way, were deficient, allows me, or at least gives me an excuse, to belabor a vital point concerning technical translating, i.e. translation of written material, allegedly nonfictional, which presupposes much relevant knowledge and relevant sophistication on the part of the ultimate human reader.

I consider my point vital enough to assign it its own paragraph. The technical translator, to be consistently correct and complete, must be a master of at least three domains:

- the *subject area*, be it a branch of mathematics or prison reform in the Third Circle;
- the *source language*, particularly (if not exclusively) as it is used by native writers actively engaged "professionally" in the particular subject area; and
- the *target language*, with the same particularity as that of the source language.

It might be objected that my point, were it adopted as the criterion for choosing, or retaining, a technical translator, would rule out *all* machine translation and many present human translators. The objection is well taken.

Let me adduce a few examples from the translations of the Chinese article in question.

- The author describes certain geometric points by an adjective (expressed by a single character) which, among its meanings, and English translations, has two nonsynonymous ones which are both valid "technical" ones in various mathematical areas. In very specific area germane to the article at issue, both the English terms show up, but with slightly diverse meanings. The character in the journal article was translated by the man by the correct English term (for the specific context), but the machine guessed incorrectly. I emphasize that the machine *guessed*. Even had the computer chosen "critical" rather than "singular," it would have had no reason for so choosing. It was the man, with his knowledge of the subject matter (and the vocabulary precisely pertinent thereto), who had *reason* to choose correctly.
- Another adjective (this time with two characters) fooled only this reviewer. The adjective occurred in the title of the article, which, you recall, was given to the computer as part of its input. The use of the specific two characters jointly to form a single adjectival lexeme is only to be found, to my knowledge, in one dictionary (published by the American Mathematical Society, no less), which gives the sole meaning of "stationary." No lexicographical source I could find gave the (human) translator's reading of "autonomous." Only by happenstance (in translating a Russian article) did I find a citation to the very current American literature which, for the exact situation at issue here, uses "autonomous." My casual familiarity with the specific field was inadequate for purposes of technical translation.
- The human translator made a correct, but infelicitous, choice of words when he wrote of a limit cycle (a geometric figure resembling a circle) "surrounding" a particular (geometric) point. More felicitous would be "encircling." The computer, however, was *wrong* on one of the two occasions and unnecessarily ambiguous on the other. (Of course, some writers, even Chinese, are sometimes guilty of ambiguity or malfeasance. Our present original writer was not.) Once, the computer had a limit cycle "outside" a point (*wrong*), and once the cycle "contains" the point. Since the "cycle" at issue is itself *made up of points*, to say that cycle X contains point Y may be saying that cycle X, as a geometric curve, *encircles* point Y, *or* it may be asserting that cycle X, as a collection of points, boasts point Y as one of that collection. To rephrase the problem: there is no ambiguity when I say that point Y is *on* circle X, or, alternatively, that point Y is *within* circle X, but what is the situation when I say that Y is *in* X?
- A final example, at least for the purposes of this overextended paper. Here, the computer dutifully, and acceptably, translated a phrase which the human, without due cause, omitted completely.

The author had said that he could, *with no loss of generality* (standard procedure and verbiage for this sort of material), set a particular symbol equal to a specific integer. Compare:

The computer: "Without loss of generality, we can take m = 1."

The man: "we can take m = 1."

The Anglophone mathematician prefers reading the assurance that generality is still secure.

(UNCLASSIFIED)

AN EVALUATION OF A SCIENTIFIC CHINESE MACHINE TRANSLATION

[redacted] P12

P.L. 86-36

Since the dawn of present-day computer science, the idea that a computer should be able to translate one natural language into another has been a most fascinating problem to computer scientists and linguists alike. A satisfactory solution to this problem, however, has proved to be most elusive. Even when the concession is made that the first attempt at machine translation should be in scientific literature, with its relatively small and precise vocabulary and usually uncomplicated syntax, as opposed to the linguistically more complex artistic literature, the solution is still far from complete. Because of the importance of machine translation and perhaps also because of the enticing nature of unsolved problems, many machine-translation projects exist throughout the world. These projects are evaluated on the quality of the translated output, as well as on the techniques employed in the translation algorithm. The Agency, with its high interest in language and language processing, keeps abreast of developments in the area of machine translation and, in line with this, I was asked recently to evaluate the translations of a new Chinese-to-English machine-translation project.

The Chinese University of Hong Kong as a computer translation project, CULT (Chinese University Language Translator), which is translating scientific Chinese into English. This project has now been developed to the point that subscriptions are being accepted for their machine translations of two Chinese journals, *Acta Mathematica Sinica* and *Acta Physica Sinica*. Plans are being made to include translations of other scientific journals published in the People's Republic of China (PRC) in the CULT service. In order to familiarize the world with this service and to demonstrate the quality of the product, the organizers of CULT have prepared a paper describing their system; the paper includes as an appendix an article from *Acta Mathematica Sinica*, accompanied by both the CULT machine translation and, for comparison, a translation by a Chinese mathematician. Also accompanying the machine translation is the form of the article at each step in the CULT process. In an attempt to evaluate this machine-translation project, I have compared the CULT translation with both the supplied human translation and my own translation.

The computer translation system employed by CULT involves only two steps before the English output is produced. These steps are pre-editing and keypunching. According to the CULT paper, pre-editing involves the addition of some Chinese words, such as understood subjects and predicates, and the flagging of dependent Chinese clauses for the machine. These additions are included so that the computer has a "complete" sentence to work with and so that the the extent of dependent clauses is known to the machine. However, in the sample article one *English* word was inserted into the Chinese text! This occurred when the original article stated "Let α, l, m, n, b be real numbers." The pre-editor inserted the English conjunction "and" into this sentence to yield the pre-edited version "Let α, l, m, n, and b be real numbers." While the insertion of English words at the pre-editing step is not mentioned in the CULT paper and its extent is unclear, this example may only be the unavoidable result of slight differences in the form of enumeration statements in Chinese and in English. One other interesting feature of the pre-editing step is the conversion of Chinese characters written in the shortened form now used by the PRC ("simplified characters") back to their more traditional form. The keypunching step is the conversion from this pre-edited form, which is still in Chinese characters, to a standard machine-recognizable form of Chinese. This form, the Standard Telegraphic Code (STC), merely assigns to each Chinese character a unique four-digit number.

The *Acta Mathematica Sinica* article chosen to demonstrate the capabilities of the CULT system states, without proof, a number of theorems in nonlinear differential equations. While both the human translation and the machine translation included in the paper were quite good, each made what I term a significant or a serious error. A translation error is serious if it is unclear what the meaning of the original article

was, based on the English translation alone. This is quite different from the kind of error where the original meaning is apparent to a person familiar with the field. The machine incorrectly translated one phrase as "[The system has a] limit cycle *outside* two singular points," whereas a correct wording would be something like "[The system has a] limit cycle *surrounding* two singular points." Realizing that a limit cycle is a kind of circle, this error is definitely serious, as the machine translation appears to make sense but is entirely misleading. The human translator also committed a significant error when he rendered into English the phrase "the sutonomous [sic] system." Even allowing for a typographical mistake which yields the much more familiar word "autonomous," this is still a serious error, as the original meaning was "the nonlinear system." While this is probably just a sloppy exchange of one technical term for another, the effect on the English-speaking mathematican is just as serious as the effect of incorrectly rendered Chinese.

One area where the human translator has an advantage over the computer is demonstrated by the machine's translation of a phrase as "a limit cycle which contains the origin," which would be more correctly translated as "a limit cycle which surrounds the origin." It might be said that this is a case of ambiguous translation since the word "contains" in mathematics can refer either to set containment (as in "3 is contained in $\{1, 2, 3\}$") or to geometric containment (as in being contained inside of a circle). I don't feel, however, that CULT should be expected to differentiate between these two distinct meanings or be criticized for not distinguishing them, because the Chinese original literally does say "a limit cycle which contains the origin." The ambiguity is in the original Chinese, not in the machine translation! The same Chinese words used here to mean geometric containment can sometimes mean set containment. The Chinese mathematician did use the unambiguous word "surrounds" in this situation, but he possessed a knowledge of mathematics and was able to use that knowledge in conjunction with his translating ability. The machine can base its decision only on the input, together with its stored dictionary, which does not include knowledge of the field of mathematics. It is, therefore, too much to expect the machine to make such a differentiation. What is required (or assumed) is that the reader of any article on nonlinear differential equations should be able to resolve the ambiguity. This is not, in my opinion, an unreasonable assumption.

Having examined this sample article and the CULT translation of an entire issue of *Acta Mathematica Sinica*, I feel that CULT could provide a quality translation of this and other PRC scientific journals on a timely basis. The question remains, however, whether a need exists in the general mathematical community for a cover-to-cover translation of *Acta Mathematica Sinica* or any other of the PRC journals. The answer to this question would have to be made by the would-be subscribers to the CULT translations.

(UNCLASSIFIED)

LETTER TO THE EDITOR

In view of the point I tried to make regarding NSA-ers' attempting to siphon personal mileage from the Vietnam tragedy ("Leo in October," CRYPTOLOG, January 1976), I can only assume from [redacted] article in April's CRYPTOLOG ("One Day in Danang: Other Duties as Assigned") that he still hasn't learned much in terms of the lessons of Vietnam.

His account of rockets, smoke, and shrapnel came across as a smokescreen not only for his lamentable lack of perception (we covered that in the January issue), but now also for his lack of good taste. Too many silenced voices will never be able to give such accounts; not to anyone, much less to a captive SIGINT readership.

I chide both [redacted] for this second, P.L. 86-36
grossly indelicate effort; and the publisher and editors of CRYPTOLOG for dignifying it as a feature article.

Respectfully,
Albert I. Murphy, V13

~~(CONFIDENTIAL)~~

. . . had a farm, E-I-E-I-O?

Here's a "Transcription in the News" item from TIME magazine (March 29, 1976, p. 24):

a very sha[illegible]dy, very shrewd."

The prosecutor also got help from a highly unpredictable source. William and Emily Harris, Patty's most ubiquitous S.L.A. companions and the only members of the guerrilla band still alive, gave a prison interview to *New Times* magazine in which Emily referred to "a stone relic in the shape of a monkey face" that Willie Wolfe once gave to Patty. "He called it an Olmec or something," she said.

That offhand remark rang a bell with the prosecutor. He recalled that on one of the tapes that Patty made during her S.L.A. sojourn she said that the "pigs" probably had "that Olmec monkey" that Wolfe—who died in the Los Angeles shootout on May 17, 1974—wore around his neck. The FBI transcribed that garbled remark as "that old MacMonkey." After reading the *New Times* article, Browning asked the FBI, on a hunch, whether Patty had a similar Olmec trinket in her purse when she was arrested. The answer was yes. That led to Browning's deft summation ploy when he wondered why Patty had testified that she "could not stand"

PROSECUTOR JAMES L. BROWNING

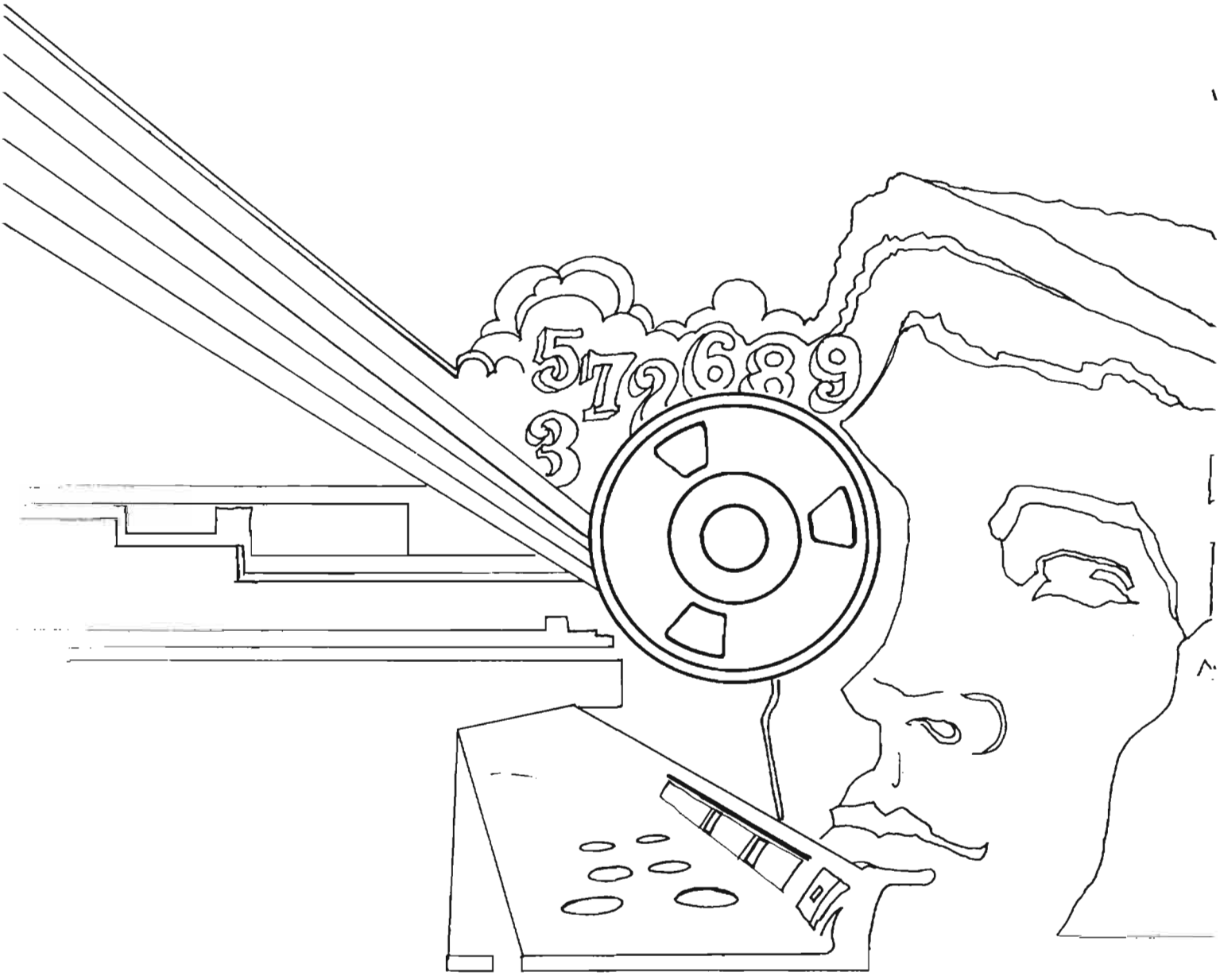
Wolfe but, long after his death carrying the tiny totem that h parently given her.

Browning contended that gan looking up for the prosecu midway in the trial—"some tween the time the judge allo introduce documents from h year [the year before her arres had to take the Fifth so many front of the jury."

What about the impact o dict on his future career? "I am I was told by some people that wanted was a federal jud shouldn't try the case. But I that I could turn over the trial to an[illegible]

[redacted] P.L. 86-36

(UNCLASSIFIED)



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~