PL 86-36/50 USC 3605

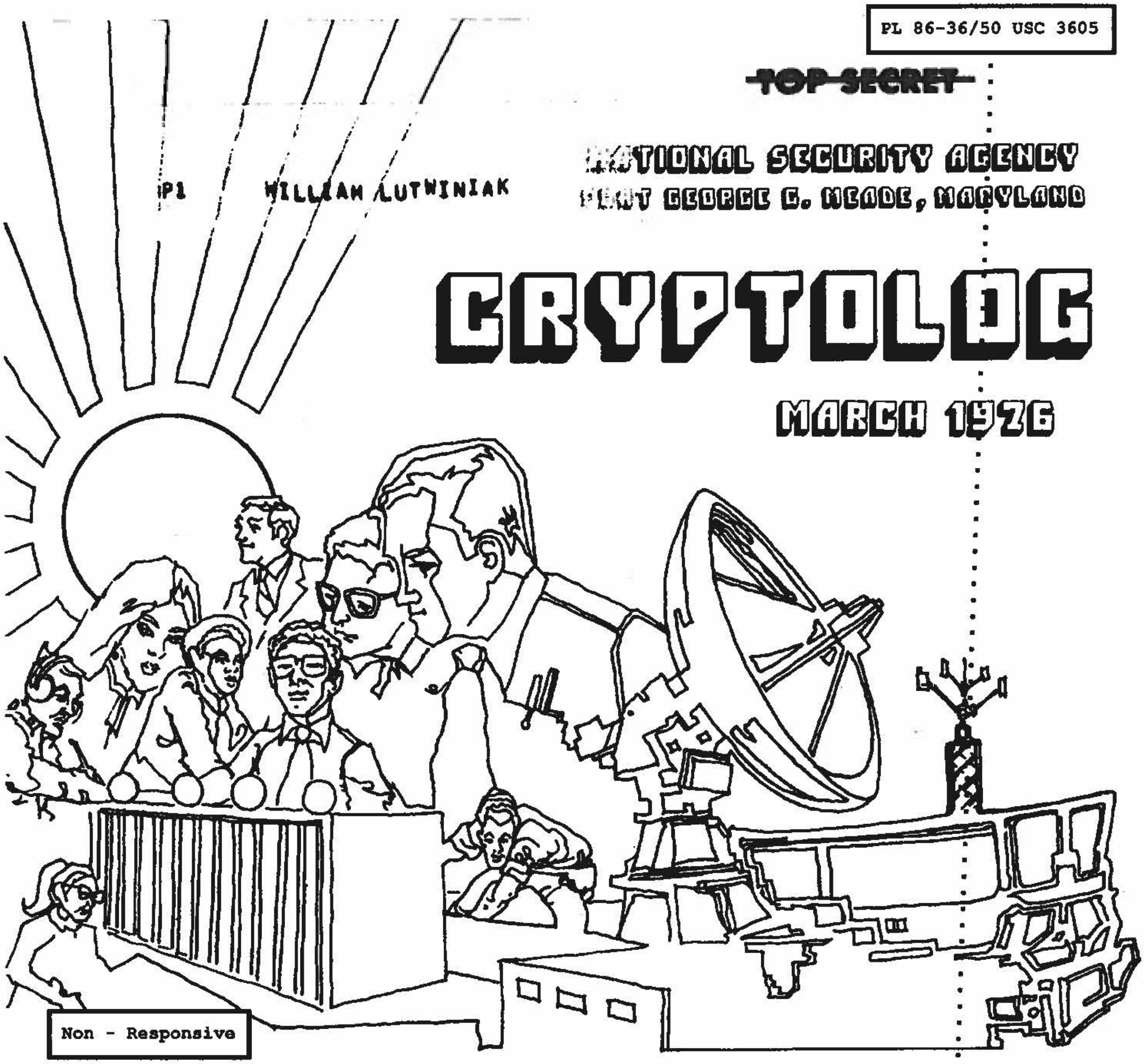
~~TOP SECRET~~

P1 WILLIAM LUTWINIAK

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MARCH 1976



Non - Responsive

~~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~~

Approved for Release by NSA on 04-26-2021 pursuant to E.O. 13526 MDR Case 109413

Non - Responsive

~~TOP SECRET~~

CRYPTOLOG

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

VOL. III, No. 3 MARCH 1976

[redacted]

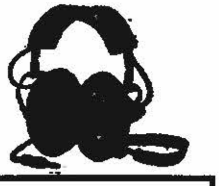
~~TOP SECRET~~

EO 3.3b(3)
PL 86-36/50 USC 3605

PL 86-36/50 USC 3605

TO PULL A "PONYAL"

[redacted] A642



It almost never fails. If the transcriber understands every word that the Russian is saying, the Russian repeats the statement several times. But if the transcriber cannot make out a word or two -- and this happens most frequently when the words are critical ones -- the Russian at the other end of the line says, *"Ponyal!"* ("Uh-huh!"), the statement is not repeated, and the conversation takes a completely different tack. Because of this fact of life, we Russian transcribers call ourselves "*ponyal* pullers," and we call the laborious job of listening and relistening to the unknown word or words, while simultaneously researching the multiple possibilities in the available research aids, "pulling a *ponyal*."

Every time that a transcriber picks up a tape, she silently prays that this one will be different. [redacted]

Going through the second time, I started to write down verbatim what the speaker was saying. I found that I had to supply inaudible prefixes or other parts of words myself. I did that either by relying on my previous encounters with the words in similar phrases, using various dictionaries to fill in the gaps in my knowledge, or by finding the phrase repeated elsewhere on the tape. For example, my experience told me that the phrase in this segment was [redacted]

But, after rebuilding as much of the verbatim utterance as I could, I was still left with one unknown stretch: [redacted] Was the unknown item a single word? Two words? The logic of the utterance called for an adjective: "The [redacted] where? It's easy to say that the missing word "has to be" an adjective, but how to prove it?

In English, an adjective (or noun used adjectivally) does not change according to the noun that follows it: [redacted] So, as I was pulling this *ponyal*, I listened for the appropriate adjectival ending. It wasn't there. I listened elsewhere on the reel for the word to be repeated: no other occurrences.

Well, then, what did the unknown item sound like? It sounded like [redacted] I looked in various dictionaries for an adjective that began that way (assuming that the ending had been spoken but was inaudible to me): no results. How about tacking on the usual adjectival endings and then looking up the possibilities in the reverse dictionaries (that is, looking for words like [redacted]? Again no results.

Okay, then, tear the word apart! Well, the combination *zk* is highly improbable in spoken Russian. Because of the feature of consonant voicing in Russian, combination of a *z* plus a *k* would be pronounced as *sk* or *zg* (even though the spelling of the word would not indicate the changed pronunciation). All right, then. Change [redacted] and check all the dictionaries again -- that shouldn't be more than a few thousand possibilities to check. Add the presumed adjectival endings and check the reverse dictionaries for [redacted] etc. -- that's only another 500 or so possibilities to check. But still I could find nothing to fit the context. Because, even though I didn't know [redacted] the speaker was referring to, I definitely knew that he wasn't discussing the [redacted] (or cut) of a dress.

Back to square one! Maybe the missing word *ain't* an adjective. I'd been thinking "along [redacted] ceded by a noun, but still nothing came close to the sounds that I heard. No, it had to be an adjective!

Getting desperate, I checked other transcripts for that date and case notation. Maybe the same phrase had been used on a different reel in a similar situation. No such luck.

EO 3.3b(3)
PL 86-36/50 USC 3605

Non - Responsive

Wait a minute! Another brainstorm! In Russian, an *l* is often misheard for an *r*, and vice versa. Not only that, but an unstressed *a* often represents an *o* in the Russian dictionary spelling (as opposed to its pronunciation). Unfortunately, the quality of my tape made it virtually impossible to know where the stress was in the unknown word. So now I had a pretty large number of additional combinations to play with: [redacted] to yield something. But, hell fire and damnation! Nothing!

What to do? Well, at this completely desperate point, another repeatedly observed feature of SIGINT life reared its head: serendipity. Have you ever noticed that after you come home from spending hours at work trying to locate a certain word, the word jumps out at you from the Tiny Taters wrapper on your kitchen counter? It happened again this time. Just as I was ready to throw in the sponge, a memo crossed my desk. One word jumped out and hit my eye -- the English abbreviation COB (close of business). For some reason it suggested to me that maybe the word I was looking for was an abbreviation itself or the first part of a telescoped word consisting of an abbreviated adjective tacked onto the word [redacted] I returned to the reverse dictionary, took the word [redacted] as my jump-off point, and then tried prefixing it with all the possible combinations I had already tried [redacted] in all their combinations and permutations), and there the word was: [redacted]

My first impression had been correct. The missing item was indeed an adjective, but it had been telescoped for brevity (the unabbreviated term is [redacted] which is much more of a mouthful). My assumption that the speaker was slurring the ending of the adjective had been wrong. The speaker wasn't using the ending of the word at all: instead, the adjective and noun had been fused into a single language unit.

This telescoping of words (also called the formation of "portmanteau words") is a very common occurrence in Russian and is not uncommon in other languages, since all languages respond to the needs and requirements placed on them. We transcribers of Russian or of other languages must remain constantly aware of the ways in which foreign languages behave like our own language. New words are being coined every day in order to meet the demands of technology and the need to communicate more and more information in less time. If it is happening in English, it is also happening in all the other living languages of the world.

[redacted]

MUSINGS ABOUT THE AG-22/IATS

Cecil Phillips, C03

The following article is reprinted from C-LINERS (C Group Machine Processing Information Bulletin), Vol. 3, No. 7, August/September/October 1975.

In November 1960, 15 years ago, the first tests of the AFSAV-D/311 (a prototype of the AG-22) were conducted at Rothwesten, Germany. At the time of the tests, those of us in the ADVA--GENS Joint Mechanization Group had great hopes that in 4 or 5 years the D-311 would have great impact on the nature of traffic analysis. We thought that the full-text input and carefully designed editing and formatting programs would eliminate much of the work of TECSUM preparation and punching of paper tapes at the site, and the card punching and editing at NSA. We realized that the results would not be as good as very carefully hand-prepared reports, but our tests showed that the average error rate of our editing and formatting programs was about the same as that of manually prepared TECSUMs.

Several recent events have sharply confirmed what I have suspected for some time, that is, the computer records generated totally automatically from AG-22 and IATS are of very poor quality. These events include detailed discussions with each of the offices in A, B, G, and W about computer needs for the future, and discussions with non-NSA elements receiving feedback from these automatic processes. The opinion seems almost universal that the output is very poor if one expects specific information such as cipher text in a format suitable for cryptanalysis. The same is true if one is looking for a unique, degarbled set of callsigns for each network. I am equally sure this applies to any kind of specific, unique information.

I do not know exactly why the goal has not been realized, but I suspect that the computer programs have not been as tightly tailored to the input as were our first experiments. There may also be more variation in the data and, perhaps, more variation in the way that it is copied. Another factor which may have been present is that our first experiments probably had the effect of stimulating the operators to copy with better than average care.

If I am right about the probable causes of the poor quality, then there are a very limited set of potential solutions for improving the results. As I see these alternatives, we can

- try to develop more precise and more sophisticated programs;
- introduce extra edit steps into the process, using interactive computer terminals; or
- make changes in the way that data is copied.

I have serious doubts about the first of these alternatives, since it would probably consume more good programmer resources than are available. The second alternative has real merit, particularly with the expected expansion of the number of available interactive terminals. However, it may also suffer from a lack of available manpower to do the editing and correction.

I believe that the third alternative -- changes in the way that the traffic is copied -- offers the best hope for the immediate future. Thus, it is my contention that we should take immediate steps to modify coding procedures, or at least to test some possible changes. The kinds of changes I would suggest are outlined below.

In the "non-message" instructions, I think that we should change the morse copying concept from the idea of copying everything to the idea of "summarizing" or something more comparable to "gisting" in voice communication. The emphasis should be on getting one good representation of the callsigns and callups, rather than all kinds of garbled versions. While it is theoretically possible to produce computer algorithms to degarble and summarize, as a practical matter a human of modest skill can almost certainly do better. Equally, the copying of chatter could be more sharply focused on unusual items by allowing the operator to give a comment on the nature of routine chatter and to copy only the unusual chatter verbatim.

I suppose that the procedures mentioned above would require some better understanding by the operators of what is important, but I can't help believing that they would be better motivated if they knew more about the targets and why they are being copied.

PL 86-36/50 USC 3605

As far as messages are concerned, I think there are some more specific things that might be done. I think the operators could do a little more to format the message. To a considerable extent the operator already formats messages. What I am suggesting is that we go as far as possible toward operator formatting. I would also couple additional "tagging" with the tighter formatting.

Unfortunately, the AG-22/KSR-37 does not permit of corrections as much as is desirable, but with TENNIS and MAROON SHIELD there are excellent possibilities for correction of copy and for production of a composite version from repeated transmissions. In any case, a strong concentration on messages might unearth other ways of producing better copy, even with the KSR-37.

There are a couple of arguments given against more tagging and more formatting by the operator. One of these is that he is already overburdened. Since I have never been an operator, I cannot deal with this directly, but it seems to me that by lessening the total amount of copy and treating the operator a little more intelligently we can certainly get a better product.

The other argument given is that the editing programs must assume missed tags and, therefore, it makes no difference whether the operator tags or not. There is some truth in this assumption, but it misses the fact that even an operator doing a poor job can put in some tags that the program can never put in. In a sense, program and operator are complementary, the program doing a better job than the operator when everything is routine, but the operator is infinitely better with any kind of variation or unique situation. To do the AG-22 job well, one needs both, and both should be as good as one can practically get.

To sum up, I believe it is time we took a drastic look at the way HF morse is copied. From what I know of COPES, a start has been made toward what is important in the trafic on a specific case or target basis. I think we can add some general goals and improve the product. At the very least, we can reduce the volume of records generated from AG-22 input and produce more useful data bases.

Comments, anyone?

Mr. Phillips was Chief of the ADVA-GENS Joint Mechanization Group, which conducted the first tests of an AG-22-like device in 1960 and 1961 at Rothwesten and Darmstadt/Zweibrücken, Germany. Carrie Berry and [redacted] *were also members of the group. The specific AFSAV-D/311 tests Mr. Phillips mentions were carried out by Mr.* [redacted]

[redacted]

Non - Responsive