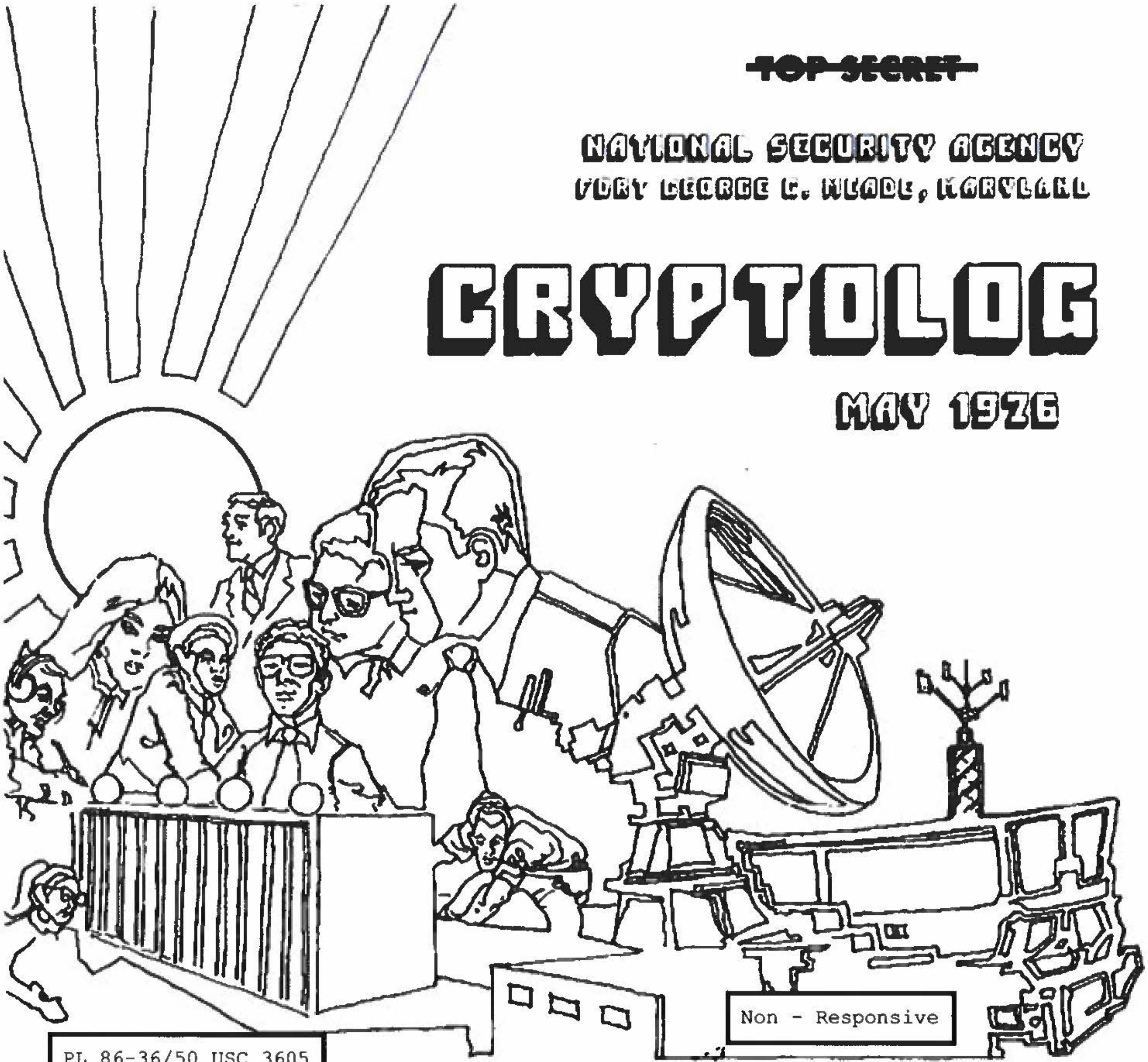
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MAY 1976



Non - Responsive

PL 86-36/50 USC 3605

~~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~~

Non - Responsive

WHAT'S WRONG WITH AG-22/IATS?

Daniel R. Connell, C7

In the March issue of CRYPTOLOG we reprinted the article "Musings About the AG-22/IATS," by Cecil Phillips, C03, which had originally appeared in C-LINERS (C Group Machine Processing Information Bulletin), Vol. 3, No. 7, August/September/October 1975. Mr. Phillips' article prompted the following reply by Daniel R. Connell, which appeared in the Winter 1976 (Vol.3, No. 8) issue of C-LINERS and is being reprinted here with the permission of its Editor, David J. Williams.

Ed.

What's wrong with AG-22/IATS? Plenty, if one accepts the thesis advanced by Mr. Phillips that the output of AG-22/IATS intercept is inferior to that previously derived from manually prepared reports transmitted to NSA.

I do not. Two of Mr. Phillips' recommendations for improving the product of ADP applications are good ones, but not because the quality of AG-22/IATS data is inferior. I maintain that the overall quality of AG-22/IATS data is better than ever, and that other forms of improvement not mentioned by Mr. Phillips are far more critical to greater utility of HF Morse.

When one speaks of carefully prepared reports being more reliable than existing data, one should not ignore the fact that manual preparation is one thing and radio transmission is another. One could take the actual message filed with the target communications center and, given hits during transmission, receive a corrupted text at the receiving end. The sender makes mistakes, also.

When speaking of pre-AG-22/IATS history, the reality was a TECSUM prepared from hard copy depicting what the intercept operator heard. Then the data was put on 5-level paper tape and transmitted electrically to NSA via either OPSCOMM or CRITICOM channels. Both forms of communications are subject to atmospheric corruption, not to mention the fact that, for either preparation or transmission reasons, the use of reperforated tape can easily become its own private nightmare. This, in fact, happened, and the word "garbled" applied to transmitted material as easily as it did to that intercepted by the operator.

The advent of AG-22 copy and STRAWHAT forwarding saw some improvement, although the quality of the final output at NSA changed little. Reperforated tape errors, although caused by different equipment, were now compounded by those resulting from faulty or dirty STRAWHAT paper tape readers. When the latter occurred, however, things were usually so bad that entire transmissions were done over. The quality of traffic received at NSA, in my opinion, probably remained the same. Unfortunately, this is still true for those materials copied on AG-22 positions and forwarded via STRAWHAT. The field stations operating in this archaic mode at the present time, however, are few in number. All the larger sites copy and forward via the Improved AG-22 Terminal System -- IATS.

IATS brought considerable change. The material copied by the operator is now implanted on magnetic tape, handled via field computer, and transmitted to NSA in an error-detection mode. Unless each transmitted bit is properly received, NSA will not accept.

It is my contention that, contrary to certain opinions expressed during planning sessions with A, B, G, and W, the quality of HF Morse intercepted on IATS positions and transmitted via that system is better than ever before. Holding that opinion, I therefore dismiss all thoughts that copy procedures, as we know them today, are the cause of "poor quality text."

I suspect that such charges emanate from various corners of classic cryptanalysis, where perfect copy from at least two sources is required by Utopian law. These same corners also exude a "message" philosophy whereby the emphasis of intercept is placed on preambles and text; callups and intervening chatter be hanged.

Even if poor quality were true, I would not subscribe to Mr. Phillips' suggestion that the operators provide more tags on their intercept. Moreover, asking them to format

~~(CONFIDENTIAL - HVCCO)~~

messages more than they do today is no way to simplify copy procedures.

It is not full copy that bothers an intercept operator. He or she is trained to copy exactly what is heard as it is heard, often under trying circumstances: bad atmospherics, radio interference, a weak transmitter, erratic keying, or just trying to keep up with one of the fastest hands in the west.

What complicates life for an operator -- and what causes the majority of copy errors -- is anything that interrupts the almost subconscious flow of intercept, any requirement for additional thought or function while intercept is underway. What Mr. Phillips suggests as a remedy to poor quality would, in my opinion, result in far less quality. I am compelled to mention that this view was paramount during the first two Generalized AG-22 Processing System (GAPS) conferences held in 1973 and 1974. From the field point of view, tagging procedures were about as popular as a full-dress review on Sunday morning. Not only do they complicate an operator's style, they adversely affect line management's flexibility in moving operators from one target entity to another, where procedural tags required by NSA can vary widely.

There is a danger, also, in having operators "gist" callsigns under live intercept conditions. Sometimes even slight variations in callups and callsigns signify the unusual, and an operator reschooled to gisting could easily become complacent or miss a unique 4-element callsign where the difference from 30 previous callups is but a single dit or dah. The same applies to asking the operator to discriminate during the listening process and copy down only unusual chatter. .

The changes in copy procedures recommended by Mr. Phillips are well suited for intercept operations where instant replay is a fact of life [redacted] The "live" AG-22/IATS operator, however, has enough to do. What is surprising is the fact that, given all that is required, the operator does a good job.

I do agree that software should check for obvious errors and, where possible, correct data when subsequent errors are detected. Extra editing steps in the ADP cycle also would prove beneficial.

Mr. Phillips' call for greater operator awareness of target signals and their value is an excellent one. One need not have been an operator to understand this. A typist is a better typist when interested in the job at hand and given informed involvement. The onus for better operator motivation falls on two sets of shoulders: those of the field managers and, as it pertains to the signals being copied the NSA elements responsible for those targets.

My experience argues strongly for greater NSA efforts to involve station personnel in the why and wherefors of intercept assignment. I speak directly of operators, not station analysts or those levels of field management familiar with end-product reports, show-and-tell briefings, and extensive exposure to visiting TDYers. Such involvement, moreover, should not be isolated but continuous. Field managers and analysts should then amplify operator interest and insure that operators are kept informed.

Before leaving the subject of operator involvement, I quickly point out that the remote intercept operations planned for NSA -- [redacted] -- offer excellent opportunity for operator motivation. If the analytic areas do not make greater attempts to keep local operators aware of the importance of their assigned mission, we will have dropped the ball too many times in our own backfield. The ideal, of course, is to stimulate operator interest regardless of where the intercept is performed.

Returning to AG-22/IATS as a source of material with which many of us work, and accepting that today's copy is of appropriate quality, is there anything associated with this intercept that should be improved -- better software and editing capabilities aside?

Those same planning sessions cited by Mr. Phillips indicated that the primary criticism of AG-22/IATS was insufficient timeliness. The resultant AG-22/IATS Processing Study Group findings show that, because AG-22/IATS is not timely enough, many manpower and machine resources are wasted by duplicative preparation and forwarding of the same intercept. At the least, resources are used which need not be used if AG-22/IATS were available to users within a few minutes of intercept.

The Study Group is still in the process of submitting a final recommendation to Chief, C, for improving the timeliness of this intercept. Doing so will not be easy, but it can be done and ought to be done. If C Group is to properly support the [redacted] activities, it must be done.

What's wrong with AG-22/IATS? It is not and never will be perfect, a replica of what the target communicator sends. The intercept associated with IATS, however, is the best we have ever had. We can always use better ADP applications. We need a faster means of getting pertinent material to interested users.

It is these needs that will continue to demand satisfaction as [redacted] and other forms of first-echelon operations develop. It is these needs, not a quest for perfect copy, that can be realized.

Non - Responsive

CONVERSATION WITH A BOOKBREAKER (SINCE RETIRED)

In cleaning out his desk, the "since retired" bookbreaker found the following text. It bore the date June 12, 1969 and the title "Suggested Topic for a Briefing (About 30 Minutes): Bookbreaking--The State of the Art." It will take less than 30 minutes to read the "conversation," but it will be time well spent by any bookbreaker.

Ed.

Q: *Can the computer be programmed to reconstruct code books?*

A: In bookbreaking, the computer only points to the answer -- it cannot be relied on to *give* it. On the other hand, the *services* performed by the computer are of inestimable value to the analyst because of the rapidity with which pertinent information can be brought to his attention. Intelligence is highly perishable -- the computer often serves to make information exploitable while it is still timely.

Q: *If the computer is not going to replace the bookbreaker, what specific services can it perform for him?*

A: One of the greatest services is in the area of inventory. Anything once known about the codes and cryptographic practices of a target country should never be forgotten. One of the most wasteful of all exercises is "rediscovering the wheel." Other than this, the computer is marvelously adaptable. With proper knowledge and imagination, it can be adjusted to fit the needs of just about any problem. The greatest danger is the growing tendency to try to *reshape* individual problems to *accommodate the computer.*

Q: *Is it likely that the "art" of code reconstruction will disappear in the near future?*

A: I should hope not. I am now working on a code that has all the basic elements of the first code problem I ever encountered -- almost 25 years ago. I should hate to think that the next generation of bookbreakers would have to learn the trade by trial and error.

Q: *What kind of training should the next generation of bookbreakers have? What kind of people should they be?*

A: Qualities of character and temperament are fully important as formal instruction in languages, area studies, or cryptography. Code reconstruction takes enormous patience, perseverance, and personal integrity. The bookbreaker must be honest with himself, or he will weave a whole web of deceit. He must have broad interests and an insatiable curiosity. Bookbreakers succeed through knowledge, *not* ignorance.

~~(SECRET UMBRA)~~

PL 86-36/50 USC 3605

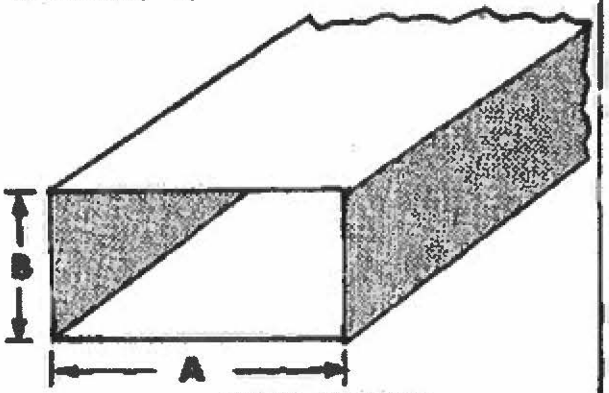
WAVEGUIDE ANALYSIS

[redacted] W222

Although it goes without saying, I'll say it anyway: before you can perform any kind of analysis on a signal, you have to collect the signal first. Before you collect the signal, you have to find it. And before you find the signal, you have to be in the right place along the radio-frequency spectrum. This is true of all signals and no less true of signals associated with modern weapons systems.

We have often known that a particular function must be associated with a given weapons system because of an associated antenna. Yet the signal associated with that function may go unintercepted for several years. When a new weapons system is first identified, there are a number of techniques to be used for predicting what signals will be associated with the system and what their frequencies will be. One method of predicting the frequency is to determine the associated antenna aperture size from photography, estimate the needed signal beamwidth for the various signal functions, and then calculate the operating frequency. This beamwidth estimation sometimes provides poor results. Another way, which is more exacting, is to employ waveguide analysis. This article shows how waveguide analysis can reduce the search range to a minimum and thus shorten the time needed to intercept the signal.

The common waveguide has a cross section that is rectangular in shape. The longer inside dimension is arbitrary called "A", and the shorter "B."



TYPICAL WAVEGUIDE

The "A" and "B" values are normally determined by comparing outside dimensions derived from photographic interpretations with U.S. waveguides in order to establish the inside dimensions. The "A" dimension determines the cutoff frequency. Frequencies above cutoff will propagate down the guide; frequencies at or below the cutoff will not. The cutoff frequency can be determined from the expression

$$F_c = \frac{C}{2A}$$

where C is the speed of light,
F_c is the cutoff frequency, and
A is the longer dimension of the waveguide cross section.

This expression is important because it reveals that the antenna associated with this waveguide cannot transmit on frequencies lower than the result. Thus, the first usable frequency range has been established: F_c to infinity.

This range can be reduced to F_c to $2F_c$, since it is known that frequencies above $2F_c$ cause the signal not to be coupled to the load properly.* The improper coupling causes standing wave patterns to be set up in the waveguide, thus degrading the signal and causing losses. For this reason, Soviet, as well as U.S., designers choose operating ranges between F_c and $2F_c$. Again, the search range has been significantly reduced.

It is now known that the antenna associated with a particular waveguide cannot transmit on a frequency below F_c and no known examples exist in which frequencies above $2F_c$ have been used.

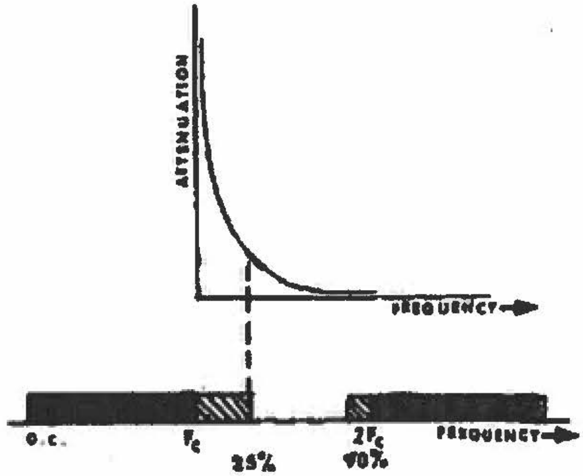
Although the search range has been narrowed significantly, there are still more factors which can help reduce the frequency search range for a particular emitter. From waveguide analysis, it is known that even though a signal can propagate through the guide at just above F_c, it is attenuated to a marked degree. As the frequency is increased toward $2F_c$, the attenuation is decreased exponentially. This usable frequency range varies from waveguide to waveguide and can be determined from a chart; however, normally the first 25 percent of the frequencies between F_c and $2F_c$ are not used because of marked attenuation. Finally, the highest ten percent of the frequencies are not used because, at about this point, the losses from the mismatching begin to become significant.

Once the frequency search range has been reduced to this range, other techniques, such as eliminating high-density bands, may complement this system and reduce the frequency range even further.

*This article is based on a TE_{10}-mode of operation.

Non - Responsive

[redacted]



TYPICAL WAVEGUIDE ANALYSIS

Although frequency prediction through waveguide analysis is not a foolproof method, it is another tool that can be used to narrow the frequency search range of a signal associated with a particular antenna whose waveguide dimensions are known. Thus, it is an important tool for speeding up the analysis of signals associated with weapons systems.

(UNCLASSIFIED)