~~TOP SECRET CANOE - SECURITY INFORMATION~~ 29 July 52

MEMORANDUM FOR GENERAL CANINE

SUBJECT: Measures for Increased Security of COMINT

1. The recent failure of USCIB members to agree on the subject proposals of the Security Committee with respect to the plain text security problem suggests the need for a fresh and possibly different approach to a solution. The tendency in the past has been to generalize on security objectives and perhaps not examine closely enough exactly what must be protected and what it is really feasible to protect. It may be well, therefore, to review our reasoning in this case.

2. In the safeguarding of COMINT which results from cryptanalytic processes (including solution of call signs and procedure systems) or from the interception of traffic which is sent in complex transmission systems with secrecy or privacy features, we have two facts to conceal: first, that we are in possession of certain information not intended for our eyes, and, second, that we are in a position to obtain more of such information in the same manner. The degree to which we must conceal these facts depends, of course, on the nature or importance of the information in our possession and the difficulties of acquiring it. In most cases, disclosure of the mere fact that we can read a cryptographic or other secret transmission system is sufficient to result in prompt countermeasures to deny us further access.

3. In the case of plain text, the situation is somewhat different. A message may be sent in clear because the sender:

a. Is not concerned with who reads it;

b. Is not aware of its significance when synthesized with other information available to the interceptor;

c. Makes a mistake;

d. Violates a regulation;

e. Has no other means of transmission; or

f. Is not aware that the transmission can be intercepted by unauthorized persons.

4. The problem of maintaining communication security from the sender's standpoint then reduces to one of exercising widespread surveillance to ensure that the foregoing things do not occur in the transmission of information which unauthorized persons must not receive. In a

(2)

COPY # 13

~~TOP SECRET CANOE~~ 29 July 52

SUBJECT: Measures for Increased Security of COMINT

vast communication complex, such as that of the Russians, this security problem is a very difficult one. If insecurity results from cryptographic or transmission system faults, a proper change in the system will correct any leaks wherever they may exist. If, however, leaks occur through plain text transmissions, it is first necessary to determine the seriousness of the leak and then the exact source or cause. The first question involves determining exactly what information is being derived by the interceptor. This will establish the latter's ability to exploit plain text traffic through information synthesization. Corrective measures can then be taken by the controlling authorities to revise regulations or procedures so that certain types of information are prohibited from being sent in clear. The second question involves determining the office of origin or the exact circuit or means by which the information is being transmitted. Only in this way can carelessness, violation of instructions, unawareness of accessibility, and similar sources of leakage be corrected.

5. If we are to combat successfully this kind of surveillance, it follows that we must deny to target nations knowledge of the results of our plain text synthesis or collation and knowledge of the precise source of information which we obtain. The general fact that we are in a position to read plain text traffic and to intercept plain text messages which are sent by channels which it is commonly known can be tapped obviously requires no special concealment.

6. Our current difficulties in the maintenance of security for our plain text COMINT operations stem principally from two facts:

a. Large numbers of personnel are required for processing, and, according to current regulations, they must be cleared and indoctrinated prior to employment;

b. The value of plain text COMINT is greatly reduced unless it can be fully synthesized with information from non-COMINT sources, because the plain text items frequently become significant only when related to other facts.

We are thus faced with the necessity of somehow reducing the number of persons that must be cleared and indoctrinated, and of somehow providing a COMINT product which can be more widely used without increased jeopardy to the source.

COPY # 13

~~TOP SECRET CANOE~~ 29 July 52

SUBJECT: Measures for Increased Security of COMINT

---

7. It would appear that at least a partial solution of the problem might lie first in a division of the work into two or more processing levels, with different security requirements for each. Thus we might regard collection (especially from open sources) and initial screening as operations which do not generally reveal the true importance of the information derived nor the exact source of specific items of importance, and, hence, as operations which do not require the same security standards as do later processes. Subsequent operations, wherein the bits and pieces are drawn together and their significance is established, are where the tight security measures must begin. In the processing of material as COMINT, it is usually essential that the exact sources be known to the analysts and security measures must be applied accordingly. This presents no special problem if the work is conducted in a COMINT agency, such as AFSA, since the same security measures are required for other operations as well. Beyond this point, however, the real difficulty arises, and there some further means must be found of lessening the need for certain of the restrictions that are now in force.

8. After processing of the material as COMINT, it has to be thoroughly collated with other material from non-COMINT sources if its full value is to be realized. Therefore, if we are to minimize the increased hazards introduced by this additional processing, two precautions must be observed:

a. To avoid pointing to kinds of information which the Russians might to their advantage bar from plain text messages, such information which is of great importance to us should continue to be handled under stringent restrictions.

b. To avoid assisting the Russians in their surveillance problem by pin-pointing leaks for them, other material should be passed out either in disguised form or without any indication of the exact origin or source (but with appropriate classification and source grading).

The latter is a common procedure in the dissemination of agent information where the precise source must be safeguarded if the agent is to remain alive. It is not unusual in the case of this type of information to withhold the name of the agent, his contacts, and the combination of the safe from which he obtained the information. Unfortunately, however, these are the very kinds of facts which are frequently demanded by COMINT consumers and which represent a serious hazard in dissemination of plain

text information. There is undoubtedly a certain amount of justification in the consumers' attitude. Nevertheless, one is unhappily forced to the conclusion at times that their demand probably results largely from the fact that there are now in the consumer agencies many ex-members of the producer agencies who are unwilling to abandon the fascinating art which they once practiced or are unwilling to rely upon the analytical powers and judgment of other practitioners. If this is indeed the case, there is some doubt as to whether these ex-producers are now in the right end of the business.

9. Obviously, any solution along the lines suggested above would require some concessions by way of compromise. The consumers would have to modify their requirements and possibly accept more material in tabulated or other summary form. The producers would probably find it necessary to change the form of certain of their reports. Prompt services would have to be afforded consumers when verification or amplification of reports is required. Some information might even be lost to consumers (although this could be a modest price to pay for maintaining the flow).

10. Whatever the case may be, something will have to give way if the present impasse is to be overcome, for we cannot have our cake and eat it too. If workers cannot use a product as required for best results, perhaps some change can be made in the workers, their work, or the materials they use. This is an approach to the plain text problem which may not yet have been adequately investigated. It should certainly be fully explored before any additional risks are assumed.

J. N. WENGER
Rear Admiral, U. S. Navy

Copy to:
Chief, Office of Operations

COPY # 13