The Borders of Cryptology

(b)(3)-P.L. 86-36

By [redacted]

~~Top Secret~~

A discussion of electronic warfare activities that are closely related to cryptology.

The cryptologic partnership in its present form has evolved from a long series of reorganizations. In the process, functions which were similar or interdependent, but separately organized and perhaps not well coordinated, were brought closer together. The togetherness was accomplished by organizational mergers and by improved liaison.

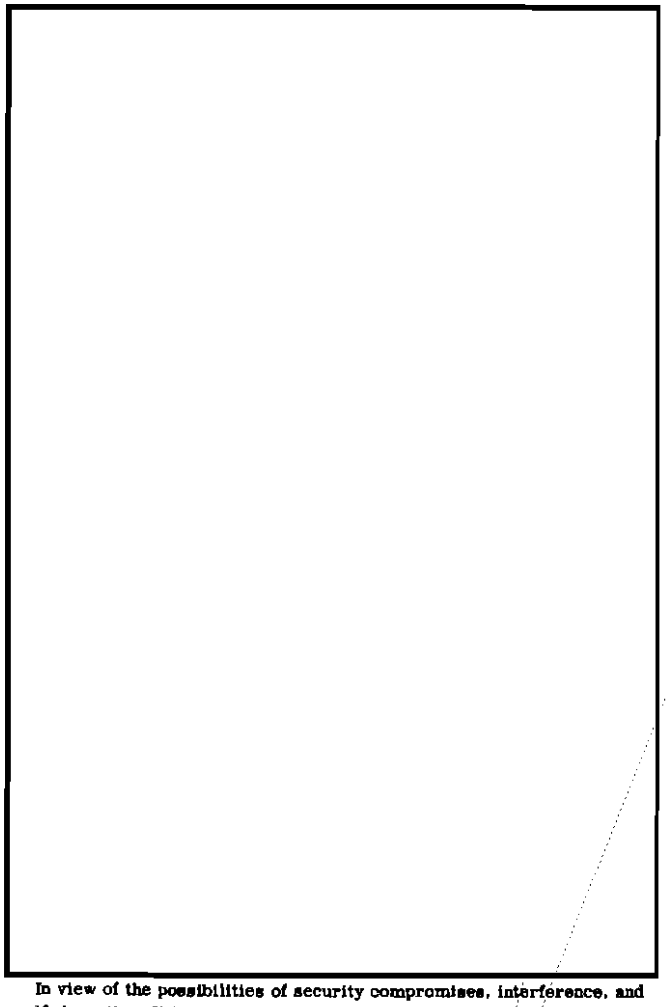
By current definition, we now have only COMINT and COMSEC activities within the borders of cryptology. On the COMSEC side, our cryptographic security and transmission security responsibilities extend to all types of electronic emission. On the COMINT side, however, a distinction is made between "communications" and "non-communications" signals. Only the former are within the province of COMINT.

ELINT activities remain outside the borders of cryptology. ELINT arrangements probably are better known to the cryptologist than the arrangements for any of the other bordering activities. In many respects, COMINT and ELINT functions are similar and interdependent; a closer organizational merger is being developed; the term "SIGINT" (which covers COMINT and ELINT) has been added to our jargon.

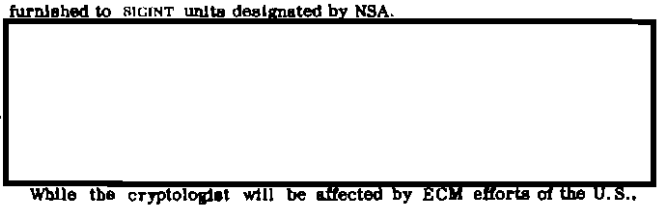
In this article, we shall consider other bordering activities which currently or potentially have an important effect on cryptology, and to which perhaps the cryptologist has not given much thought. Those activities are jamming and electronic deception in particular, and electronic warfare in general.

Although we may observe that certain electronic warfare activities and cryptology or SIGINT are similar and interdependent, we do not intend to raise here any questions of further reorganization. From our broad review of current relationships, however, we should recognize at least the potentialities for close liaison among the bordering activities.

The two major subdivisions of electronic warfare are electronic countermeasures (ECM), and electronic counter-countermeasures (ECCM). Jamming and electronic deception are examples of *active* ECM. Search, intercept, D/F, range estimation, and signal analysis, when conducted for *steerage* of active ECM, are examples of *passive* ECM. The steerage of a jamming operation, for instance, would include the transmission frequency and identifying characteristics of the signal to be jammed. The term ECCM covers anti-jamming or anti-deception measures.



In view of the possibilities of security compromises, interference, and self-deception, U.S. communications jamming and imitative deception operations are subject to USIB approval in advance. USIB has specified circumstances in which this advance approval has already been given. USIB has also prescribed the conditions for conducting an operation when time does not permit the obtaining of advance approval. NSA is required to arrange for military commanders to be advised of the status of approval for a given operation. In addition, NSA is required to arrange for the necessary SIGINT support. While SIGINT units would give, they would also receive. When SIGINT activities are performed outside the scope of NSA's authority, there would be an arrangement whereby the results would be furnished to SIGINT units designated by NSA.



While the cryptologist will be affected by ECM efforts of the U.S., he will also play an important role in those situations in which the U.S. observes or is the victim of foreign ECM. The COMSEC specialist participates in the development of anti-jamming measures. He develops authentication systems and other anti-deception measures. Interception and analysis of foreign ECM signals is a SIGINT task. The analysis of foreign imitations of U.S. signals, however, would concern the COMSEC specialists more than the SIGINT people. The latter would be concerned with technical studies of jamming signals and with techniques for seeing through manipulative deception.

Electronic warfare activities have little noticeable effect now upon cryptologic or SIGINT activities. The Soviet signals which jam the Voice of America have been subjected to thorough technical analyses by ELINT activities. Aside from the extensive Soviet jamming of the Voice of America and of similar broadcasts by the West, there is practically no evidence that active ECM operations are being conducted now by the Soviet Bloc or by the West. Active ECM operations by the U.S. are limited in view of the various risks mentioned above and the high-level controls which call for special authorizations. Similar controls have been established in the electronic warfare policy of NATO. In addition to the risks we have mentioned (e.g., the possible loss of SIGINT security, or the possible interference with SIGINT collection), there is the danger that increased

active ECM operations by the West now would stimulate greater use of active ECM by the Soviet Bloc.

Although current use of active ECM is limited, much effort must now be devoted to electronic warfare problems. We should not attempt to predict here the solutions to the problems, but we should mention some of the major issues which would affect cryptology.

The electronic warfare policy promulgated by the Joint Chiefs of Staff provides for the development of an effective ECM capability. Similar provisions are contained in the NATO electronic warfare policy.

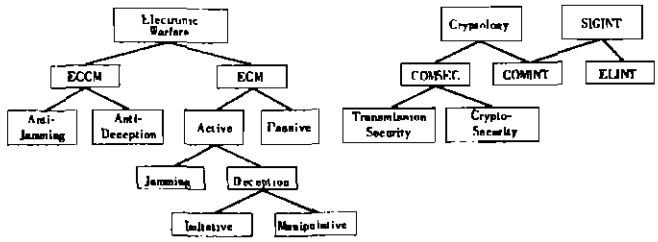
The development of an effective ECM capability implies the readiness of active and passive ECM specialists, suitably trained and equipped to handle operational tasks on short notice. Several NATO countries look to the U.S. for assistance in training and equipping units for active and passive ECM. It is difficult to provide for realistic training in passive ECM without revealing sensitive technical SIGINT information.

The problems of assisting in the development of an allied country's ECM capabilities are considerably more complex than those encountered in the development of U.S. capabilities. The complicating factors include the U.S. restrictions on COMINT, ELINT and COMSEC collaboration with foreign countries. The problems are also complicated by the several fundamental differences which are indicated in individual nations' views on COMINT-ELINT-COMSEC electronic warfare relationships. If our present restrictions were to be relaxed, the risks of compromise of course would increase, but we would be in a position to advise the recipients on security principles. If our restrictions were to be maintained, we might expect several NATO countries to exchange their sensitive technical information in arrangements which would exclude the U.S. In that event, the information might be handled under increased risks of compromise without the benefit of U.S. advice on security principles. Among the fundamental differences of views on COMINT-ELINT-COMSEC electronic warfare relationships, some NATO countries have expressed the view that passive ECM units should not only be trained and equipped, but also operational now; that they should contribute to an international exchange of electronic warfare intelligence.

While fundamental differences may exist in individual nations' views, there are also problems within the U.S. on the matter of determining details of COMINT-ELINT-COMSEC electronic warfare relationships. The exact borders of cryptology may often be questioned. Attempts have been made to draw the line according to raw materials or processes, but those attempts have not been completely successful. Having decided, for example, that COMINT and ELINT are distinctive, we can easily illustrate the distinction in terms of radio-telegrams and radar signals. We might have some difficulty, however, in determining whether a new type of signal from an earth satellite vehicle is in the province of COMINT or ELINT. As far as processes are concerned, we might attempt to place within the borders of cryptology the "specialized" processes in crypto-mathematics, crypto-linguistics, etc., but on close examination some of the specialized processes are borderline. They resemble work done in non-cryptologic areas of government, industry, and educational institutions.

[redacted]

The bordering activities which we have considered are summarized below in chart form. The chart probably takes in all of the main subdivisions in the electronic warfare complex, but we are not absolutely certain that it does. We know, for example, that active ECM *includes* jamming and deception; if there are other types of active ECM, we do not know what they are.



In our comments here on existing relationships among bordering activities, we are criticizing and applauding as little as possible. But it must be apparent that these relationships are not perfect. Not all significant issues have been settled yet. Some which have been settled are still not easily understood. Some which may be understood do not seem entirely

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

logical. The imperfections cannot be traced to flaws in a master plan for the related activities; there is no such plan. The authorities who drew up national policy on COMINT, ELINT, and COMSEC were not the same as those who developed electronic warfare policy. The need for a master plan was not apparent when the separate policies were budding. Good progress has been made, especially during the past few years, by the several authorities concerned toward satisfactory settlement of individual issues. The progress is likely to continue by working on individual problems instead of attempting to solve them all at once by drawing up a master design now.

We have indicated the potentialities for close liaison among the bordering activities. The individual cryptologist may wonder what his own role will be. The liaison channels are still in an early stage of development. Relatively few cryptologists have been designated to conduct such liaison. As the number grows, the individual's duties will be apparent in technical instructions, terms of reference, appointments to panels, etc. The majority of cryptologists may never be designated to perform a liaison function, but they may nevertheless expect to be assigned some tasks which will support electronic warfare activities, or to be consulted by liaison people on some aspect of those activities.