(E). Relationship between Communications intelligence and Cryptographic Security

20. Successful communication intelligence operations cannot be conducted without adequate cryptographic security. Cryptographic security processes and activities are complementary to communication intelligence processes and activities, and the adequacy and efficiency of the former are enhanced by the successes achieved in the latter. Gains made in the latter provide safeguards to be applied to the former. Similar talents and activities are required in both. Efficiency in the Federal Government requires coordination and supervision within each field, but it is not essential that this coordination and supervision be exercised by the same agency.

DISCUSSION

21. Although cryptographic security policy determinations and processes are to some degree related to communications intelligence activities, they are not inseparable. It is true that information is furnished from communications intelligence sources which leads to enhanced security of our cryptographic systems. It is also true that intelligence from other sources, such as captured documents and prisoner of war reports, leads to enhanced security of our cryptographic systems. However, the degree of security attained in our cryptographic systems does not depend entirely upon intelligence sources. Information derived from purely technical cryptanalytic studies made by the cryptographic security personnel themselves is much more important. In fact, secure cryptographic systems can be and in the Army and the Navy have been established by an entirely theoretical approach not involving communications intelligence or other intelligence activities.

22. In establishing and maintaining cryptographic security the approach is from the communications point of view, whereas the approach to the production of communication intelligence is from the intelligence point of view. Although, in general, similar talents are required of the personnel engaged in certain of the purely technical operations involved in both cryptographic and cryptanalytic activities, nevertheless, because of the differing points of view noted above and because of differing procedures for handling the final products of these two

activities, separate staffs have been deemed necessary. Hence, although in both the War Department and the Navy Department responsibility for cryptographic security activities and for cryptanalytical activities are vested within single organizations in each of those Departments, the actual work involved in carrying on these two activities is performed by separate staffs therein.

23. For security reasons, segregation of these two functions and personnel is advisable. The danger of drying up communication intelligence at the source, unless the activities and results are safeguarded by rigid restrictions and unless a curb is put upon the desire of many agencies to engage in such activities, has been adequately recognized by the fact that by Presidential directive cryptanalytical activities of the Government have been limited to the Army, Navy, and FBI.

24. Studies having as their aim the protection of our own communications are affected by cryptanalytic studies on foreign cryptographic systems, and techniques derived from the latter provide valuable information for the improvement in the security of our own communications. Hence, any communication intelligence relating to the security of our own communications should be made available to all the personnel responsible for communication security. A permanent supervisory agency to insure the security of cryptographic systems and related procedures throughout the Federal Government should, if properly constituted, include members having access to communication intelligence in order to insure that such intelligence would be made available to the personnel responsible for cryptographic security.

25. Cryptographic security activities should not be so closely integrated with communication intelligence activities as to preclude independent functioning of any supervisory cryptographic security policy board which might be established for the purpose of establishing and maintaining security of Governmental communications. Cryptographic security should and must be prepared to stand on its own solid technical foundation, without aid of communication intelligence, because the existence of the latter depends upon rather slender threads which may be cut at any time and without notice. Hence, if security of our own communications is to be assured under possible future contingencies involving our inability to derive intelligence relating to our own.

communications from the study of foreign traffic, either because the cryptographic systems encountered cannot be solved or because communications intelligence activities as a whole are suppressed, it is obvious that reliance should be placed not upon the questionable continued availability of communications intelligence but rather upon setting up cryptographic security staffs and activities independently of communications intelligence staffs and activities.

26. If a Board having jurisdiction over policies applicable to cryptographic security and related procedures is established it does not follow that the functions of such a Board should be expanded to include jurisdiction over communication intelligence matters. A single Board for these two related activities is not necessary for the most efficient functioning of either activity, nor for security reasons, is it advisable.

27. It should be noted that despite the fact that in the British Government there is a complete integration of cryptographic compilation, cryptographic security, and communication intelligence activities within a single organization (GC and CS), nevertheless that Government has recognized the necessity or desirability of separating the control of cryptographic security activities from that of communication intelligence activities. Two separate boards have been established for this purpose, (1) the Signal Intelligence Board and (2) the Cipher Policy Board. One interlocking membership to coordinate the functioning of the two Boards is provided.

28. If a permanent board is found to be necessary or desirable for controlling the communication intelligence activities of the Government, the informal Army-Navy Communications Intelligence Coordinating Committee, now in existence for the purpose of coordinating communications intelligence activities of the Army and the Navy, is the proper agency to make recommendations, at an appropriate time, for the establishment of any such permanent board.