Orig. with attached papers - Col Akin's office
1st copy - Maj. Wilson (with attached papers)
2nd " - hers
3rd " - hers } no attached papers
4th " - hers

SECRET

SPSIS-3

22 September 1944.

8

MEMORANDUM for Director of Communications Research.

Subject: Proposal for an ABC Committee.

1. It is believed that there is a great need at the Signal Security Agency for a thorough and complete integration of certain activities of B Branch with those of A and C Branches. This Agency is charged with the responsibility of providing security for Army communications. Let us set down the functions of the Chiefs of the Security and Intelligence Divisions as set forth in the Organizational Manual of 21 August 1944.

"Section VII--SECURITY DIVISION

44. Chief - Directs, supervises, and coordinates action relating to signal security, radio countermeasures, and security regulations of the War Department Traffic Security Board; establishes policies governing the development and production of, and operates certain signal security facilities; coordinates matters concerning security publications which are not cryptographic systems or integral portions thereof; maintains liaison relative to cryptographic matters with other Arms and Services, the Navy, and friendly foreign powers; directs preparation of technical training material; coordinates the activities of the Division; does not maintain an office of record."

"SECTION VIII--INTELLIGENCE DIVISION

48. Chief - Exercises general supervision and coordination over all activities concerned with deriving intelligence from the intercept of foreign cryptographed communications; conducts the necessary liaison relative to cryptanalytic and associated matters with other Arms and Services, the Navy and friendly foreign powers; provides for special in-job training for personnel engaged in cryptanalytic and other duties concerned with the production of intelligence; prepares technical training courses and material; initiates development of special equipment through Security Division; does not maintain an office of record."

2. No where in the Manual is there provided any method for coordination of these two Branches for the specific purpose of making more secure the communications of the Army. There is a certain amount of liaison that takes place, of course, but this at best is only a hit and miss method, guided wholly by individual resourcefulness and accident. There is incorporated in these

SECRET

Lab B

Divisions two diametrically opposite points of view from the standpoint of the science of cryptography and cryptanalysis. In the Security Division there are practicing cryptographers and theoretical cryptanalysts, but there are just the opposite in the Intelligence Division. Thus in the former they prepare cryptographic systems and then study their security from a theoretical point of view, and they must be prepared to outwit and keep one or more steps ahead of the world's greatest foreign cryptanalysts. On the other hand, the Intelligence Division takes the cryptographic output of the world, analyzes it, constantly probing for weaknesses, and always strives to outwit and keep ahead of the world's greatest foreign cryptographers. It has always been considered that a cryptanalyst must be a higher trained specialist than a cryptographer, yet we place more emphasis on personnel to outwit foreign cryptographers than on those to outwit foreign cryptanalysts! That is to say, we are more concerned with getting information from foreign communications than of preventing our own from being read by foreigners.

3. When the organization was small, the two functions, cryptography and cryptanalysis, were concentrated in the same people, but mushroom growth has segregated them into two entities in direct proportion to the growth. The emphasis on cryptanalysis naturally was on enemy and other systems, and personnel for this purpose necessarily were compartmented in B Branch. The cryptographic branch suffered as a consequence. A gauge to this situation is shown by the fact that at the present time the T/O of B Branch calls for 1 P-7, 8 P-6, 22 P-5, 112 P-4, etc., while C Branch's allotment is 4 P-4, 12 P-3, etc. The point here is that it has apparently not been considered necessary to assign the higher P ratings to C Branch, and as a matter of fact their highest actual rating at present is P-3, of which there are 2. In addition, there are 6 P-2's and no P-1's.

4. The Security Section of C Branch and A Branch should have the greatest interest in the output and operations of B Branch, first, to discover what the foreign cryptanalysts and traffic analysts are doing with ours and other nations' systems as revealed in the Bulletin; second, what cryptographic methods are used by foreign nations; and third, what cryptanalytic and traffic analysis procedures are used in B Branch that can be of use to A and C Branches in the study of our systems and methods. Unless every scrap of knowledge gained in B Branch which can be of possible use to the security of our own communications is used for that purpose, then the mission of the Agency is not being fulfilled.

5. Certain manifestations have demonstrated the need for more integration. Some of these are as follows:

a. The C Bulletin series, apparently so called because they were of interest to C Branch only. These concerned at first foreign knowledge of U. S. cryptographic systems. Probably at

first they were intended to apprise C Branch of compromise of our systems, and at first included only such material. This series now includes traffic analysis studies on our communications and the reading of codes of any country. The distribution of this series in C Branch is limited to the front office.

b. Studies of the security of the CCM to which several experts from B Branch were called.

c. Conferences on the use of the SIGCUM for "one-time" use to which experts of B Branch were called.

d. Conferences on security of the Strip device and of the M-325 indicator weakness in which there were also B Branch personnel.

e. Indicator descriptive studies from B Branch made available to C Branch at the instance of the Office of the Director of Communications Research.

f. An A Branch course in U. S. traffic analysis in which is incorporated a chapter on Japanese T/A supplied by B-IV section which is written mostly in Kana.

g. Transfer of Captain Raskin from B to C Branch Security Section.

6. All of the above are isolated incidents with no general plan in mind. Improvements in the present arrangements can be made and new arrangements studied.

a. For instance the C series should be shorn of all Japanese terminology so that C and A Branches can readily understand them; in addition, this C series should be given wider dissemination in the Security Section of C Branch and in A Branch so that overall studies may be made. An example of the kind of study that should be made is shown in Tab A. This combines U. S. operational reports with information about U. S. operations gleaned from Japanese messages of the C series. This paper was made from two independent research studies in B-I Section and the Office of the Director of Communications Research.

b. The study of the Japanese Signal Intelligence Service, now about to go into a third edition, being undertaken in the Office of the Director of Communications Research, would be an ideal job for the Security Section of C Branch. Another study from the German viewpoint should also be undertaken. There is much material on this problem from British sources.

c. All of the code instruction messages of the Bulletin should be made available to the Security group also. These are a

continuing demonstration from actual operations of lessons in cryptographic security, indicator weaknesses, etc.--"operational do's and don't's".

d. If and when a complete Japanese cryptographic history is prepared in B Branch, certainly representatives from Security Section of C Branch should participate.

e. Problems arise where it is necessary to determine the extent of compromise of our own systems in various instances and to consider to what extent security must be sacrificed consistent with practical and efficient field operation of our own cryptographic systems.

f. How can the techniques of B-IV traffic analysis operations be applied to our own communications? Perhaps a complete exchange of personnel is necessary.

g. Complete systems studies prepared in B Branch should be studied by Security Section of C Branch, as well as all cryptanalytic technical papers. New ideas and a fresh point of view would result.

h. Study and evaluation of present security studies, instituting changes where necessary.

7. These are only some of the possibilities and further study and thought should produce more. It is recommended that a permanent committee be set up to consider these problems and others as they arise, and to determine what further steps in integration are necessary. It should have the power to appoint special "working groups". Members of the committee should be substantially as follows:

Commanding Officer, S.S.A., ex officio.
Director of Communications Research, Chairman.
O.I.C., Security Division.
O.I.C., Intelligence Division.
O.I.C., B-II.
O.I.C., B-III.
O.I.C., B-IV.
O.I.C., Traffic Analysis, A Branch.
O.I.C., Security Section, C Branch.
O.I.C., Cryptanalysis, C Branch.
Any additional technicians deemed advisable such as Ferner, Small, Jacobson, and representatives from F Branch.

MARK RHOADS,
Assistant Director
of
Communications Research.