TOP SECRET

SPSIR-1 16 May 1945

SUBJECT: Study of Cryptanalytic Agencies

TO: Chief, Special Distribution Branch
2C 844, The Pentagon
ATTENTION: Chief, Special Branch

1. The attached letter from Captain Howard outlines the principal types of material available in SSA bearing on the proposed study of cryptanalytic agencies.

2. This preliminary survey suggests that even a respectable beginning of the study would require a tremendous amount of work and the services of a substantial research and clerical staff.

3. The Assistant Commandant has seen the inclosed letter and has cleared it for submission, in whole or in part, through the Intelligence and Security Subcommittee of ANCICC. Inasmuch as I shall miss the May meeting I am forwarding it to you to be handled in whatever manner seems appropriate.

FOR THE COMMANDING OFFICER:

1 Incl
Ltr from Capt Howard
16 May 45

JOHN H. CONNOR
Major, Signal Corps
Chief, Information & Liaison Branch

COPY

Foreign Cryptanalytic Spec. Acc.

TOP SECRET

TOP SECRET

SPSIR-1

15 May 1945

SUBJECT: Available Material Concerning Other Cryptanalytic Agencies

TO: Chief
Information and Liaison Branch

1. Following is a brief check-list of materials available at SSA which would be useful in appraising foreign cryptanalytic agencies in accordance with the directive of ANCICC 16 April 1945. Materials are listed by cryptanalytic centers under the SSA branches where they are available:

I. B II Branch

A. GC and CS

1. Progress Reports, Japanese Military Ciphers. Numbers 5-18, inclusive, except numbers 6, 8, 12; dated monthly from September 1943 - March 1945. These reports embody technical information such as recovered keys, additives, and squares for Japanese Army Code systems, together with some T/A results. These are important as indicating systems emphasized, individual achievements, and technical methods. These reports are expected to continue at monthly intervals.

2. Weekly Reports from SSA liaison officer (Captain Rupp) at GC and CS. These are dated from December 1944 - April 1945. They contain a certain amount of technical information comparable to that contained in the Progress Reports together with some description of organization and facilities (e.g., IBM at GC and CS is about 1/3 as large as at SSA). Of secondary importance.

3. Ultra JM Crypt Weekly Reports. Beginning February 1944, embodying CI information. Of small value for the purposes of the projected study.

4. Miscellaneous technical information embodied

TOP SECRET

in irregular reports.

5. Miscellaneous intelligence information in various documents. This material has been forwarded through the British Liaison Officer at SSA. It consists in Order of Battle Information, specialized language dictionaries, gazetteers, and a little shipping information. It is largely intelligence dervied from non-ultra sources.

B. WEC

1. Monthly "C" Section Report. Usually issued semi-monthly. Complete from May 1944 - April 1945. Contents similar to those of GC and CS Progress Reports. These reports are photostated, and duplicates are filed separately according to systems discussed.

2. WEC publishes from time to time reports of an intelligence nature. The best example at present available in B-II is entitled "JAAF in the SE Asia Area," containing a detailed account of Japanese air strength and movements in the area.

3. An E Branch report, "Value of WEC Traffic," is on file in B-II. It provides a picture of WEC's place in the world intercept organization.

C. CBB

1. Monthly Progress Reports, February 1944 - March 1945. Similar to GC and CS Progress Reports.

2. Reports from SSA Liaison Officer (Captain Fuld). These began 31 March and more will be forthcoming. They are very comprehensive, embracing not only technical data, but personalities and physical layouts.

D. Considerable material can be secured from interviews with B-II personnel who have visisted foreign centers or worked with foreign cryptanalysts. Such interviews can be arranged through Major Swears.

II. B III Branch

A. GC and CS

1. Reports from technical personnel sent from B III to GC and CS. A considerable number of such reports exists, covering a period of two or three

years. They contain not only technical data but also information as to organization (e.g., organizational charts submitted by Capt. Fried), administration, and personalities. Overall evaluations of cryptanalytic achievements and future potentialities are available in these reports.

B. Other Governments

1. The only other material seemingly available in B-III is a document on German, Italian, and Rumanian cryptanalytic bureaus. This document is on file in Information and Liaison Branch and will be described among Information and Liaison material.

C. Suggestions

1. Colonel Rowlett and Captain Fried discussed sources with the writer, among which were the following:

a. "C" messages. Most of these are consolidated in the report on file in Information and Liaison Branch.

b. "TICOM" reports to Colonel Hayes. These are concerned with European Axis cryptanalysis.

c. Personal knowledge of B-III personnel.

III. Information and Liaison Branch

A. Axis Cryptanalytic Bureaus

1. One document filed in IR-7 (ER 61994) contains detailed interrogations of a number of Italian Signal Intelligence personnel. A good general account of the Italian cryptanalytic bureau (SIM) up to the time of the armistice can be obtained from it. This would include technical achievements, personalities, organization, and sufficient material on which to base a fairly accurate judgment as to the efficiency of the SIM. The interrogations give a few facts concerning cryptanalytic achievements of such other nations as Germany and the Balkans.

2. Another document (IL 3888 D) is similar, providing additional information of the same type.

3. A complete report on the Italian cryptanalytic agency written by a former officer of the agency, has lately been distributed by IS-1. A copy is on file in IR-7. In conjunction with the documents noted above, it should provide all the important material needed for investigation of Italian cryptanalysis.

4. Three other documents (CSDIC (UK) SIR 1335; CSDIC (UK SIR 1106; SCDIC CMF Y3 A51672) are registered in IR-7, but are at present unavailable. Resumes of their contents filed in IR-6 indicate that they are comparable interrogations dealing with the German cryptanalytic bureau.

5. A report prepared in October 1944, "Cryptanalysis by Foreign Nations," is on file in Information and Liaison Branch. It was compiled largely from "C" messages in the SSA series. It discusses Japanese Finish, German, Turkish, and Italian cryptanalytic activities in as much detail as possible, and lists "C," "D," and "L" messages mentioning such activities in Great Britain, Hungary, and Russia. Messages on the same subject received since October are on file in Information and Liaison Branch and should be surveyed to bring the report up to date.

IV. Office of the Director of Communications Research

A. Japanese Cryptanalytic Bureau

1. An extensive report (3d ed) on Japanese cryptanalytic activities, compiled by Mr. Rhoads, is on file in this office. It combines all material available as of 1 November 1944, and contains a complete bibliography of sources. It seems likely that this report embodies all relevant material available at SSA up to 1 November 1944.

B. German Cryptanalytic Bureau

1. "Y Service Report" from GC&CS, undated, probably late in 1943. A comprehensive study, comparable to the report on Japanese activities except for its obsolescence.

2. Supplementary to the report is a list of perhaps 15 documents, mainly prisoner interrogations, which should serve to bring it more up to date in most particulars.

TOP SECRET

C. Miscellaneous

1. The miscellaneous file of the office contains a few letters and short reports on foreign cryptanalysis which might prove useful in filling in gaps in knowledge procured from other sources. One report contains a few paragraphs about Polish cryptanalysis.

2. A few miscellaneous documents are listed by Mr. Rhoads. The only one of much importance is WD 137593, a short discussion of Swedish cryptanalysis.

2. It seems evident that the material at hand is insufficient for carrying out the directive. It is probable that a cryptanalyst could make excellent reports on GC&CS, the German "Y" Service, and possibly the Italian SIM. Evidence as to Japanese activities would probably leave much of importance unknown. Thus, only one nation high on the priority list could be satisfactorily studied. It is believed that these studies would entail considerable time and effort.

EDWARD G. HOWARD
Captain, Signal Corps

TOP SECRET