~~TOP SECRET~~ TOP SECRET U.S. EYES ONLY Register No. 2

Staff Study

on

REPLACEMENT OF THE COMBINED CIPHER MACHINE

Prepared by

AFSA-04 and AFSA-14

in Collaboration with

Dr. A. Sinkov
Mr. [illegible]
Mr. [illegible] Austin
Mr. [illegible]

24 June 1950

This represents final paper supported not only by AFSAC listed here but also by Col. Collins, Capt. Wenger, Capt. Shepard, Dr. Kullback, etc. - all in unanimity except Capt. Safford, Cmdr. Seiler, & of course Adm. Stone. J 15 June 50

TOP SECRET - U. S. EYES ONLY

REPORT BY THE ARMED FORCES SECURITY AGENCY COUNCIL
in collaboration with the JSEC
to the
JOINT CHIEFS OF STAFF
on
REPLACEMENT OF THE PRESENT COMBINED CIPHER MACHINE (CCM)
References: JCS 2074 Series

THE PROBLEM

1. To draft, for approval of the Joint Chiefs of Staff, a reply to the memorandum by the Representatives of the British Chiefs of Staff, BMM 1/46 dated 14 February 1950 (JCS 2074/3), regarding the feasibility of constructing an adaptor for U. S. use which will permit intercommunication with the new British cipher machine.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

2. See Enclosure "B".

CONCLUSIONS

3. It is concluded that:

a. As to the feasibility of constructing an adaptor for U. S. use which will permit intercommunication with the new British cipher machine, the problem should be considered separately for each of the two proposals outlined in Encl B above.

b. In case Proposal A were adopted, an adaptor for the [illegible] (on the basis of 7-rotor [illegible] principles) and a 7-rotor [illegible] machine would have to be developed, service tested, and procured by the U. S. The U.K. would have to develop, service test and procure an adaptor for their machine. It is probable that the construction of such an adaptor is feasible, although U. S. technicians are not certain as to this point.

c. In the case of Proposal B, neither a special adapter nor a separate machine would be necessary for either country. However, it would be necessary for the U. S. to disclose to the U.K. certain specific detailed

CONCLUSIONS (Continued)

g. (Continued)

information concerning the ECM/SIGABA. This would entail a modification of a previous decision of the U. S. Joint Chiefs of Staff. In this regard, reference is made to JCS 2074, dated 25 October 1949, in which it was maintained that the U. S. must reserve for itself a cipher equipment of assured security to provide privacy for its own communications. Modification of this decision is warranted by the fact that there is no longer any doubt that the British are aware of the basic and most important ECM/SIGABA principles and intend to incorporate them in their new machine.

d. The cost to the U. S. of the adoption of Proposal A would be at least $6,000,000. The cost of Proposal B would be not in excess of $100,000.

e. In the light of the serious disadvantages of Proposal A both to the U.S. and to the U.K., and the doubtful advantage to be gained by the U.S. in any longer withholding only some minor details of the construction of the ECM/SIGABA, Proposal A should not be made to the British Chiefs of Staff.

f. In the light of the many advantages of Proposal B both to the U.S. and to the U.K., and the certainty of the U.S. avoiding unnecessary expenditure of a large sum of money, Proposal B should be made to the British Chiefs of Staff.

g. Even though Proposal B were accepted and the U.K. were to continue with the development of the new machine, it would still be feasible to withhold some of the minor specific wiring details of the ECM/SIGABA until a satisfactory test has been completed, using substitute information for that which would be withheld until the practicability of intercommunication had been demonstrated.

h. Regardless of which proposal is adopted, the U.K. should be requested to design their machine so as to use the same size rotor as that used in the ECM/SIGABA.

RECOMMENDATION:

4. It is recommended that the memorandum in Enclosure "A" be forwarded to the Representatives of the British Chiefs of Staff.

TOP SECRET

ENCLOSURE "A"

MEMORANDUM FOR THE REPRESENTATIVES OF THE BRITISH CHIEFS OF STAFF

1. The U.S. Chiefs of Staff have studied the drawings of the new British machine submitted as an enclosure to RDC 1/48 dated 12 April 1950, and have ascertained that intercommunication between a U.S. machine and the new British machine would be feasible provided certain details are incorporated in the British design. These details would not affect the use or security of the British machine for intra-British communications and at the same time would permit its use for Combined Communications on all levels where such a machine would be issued. In essence, the new CCM would have five (5) active rotors in the alphabet mase and four (4) in the control mase, without the use of a special cipher unit.

2. The U.S. Chiefs of Staff will provide the British Chiefs of Staff with the engineering details necessary for this purpose at such time as the U.K. is ready to begin the construction of a prototype model of the new British machine. Subsequently, service tests involving Combined Communications can be made, and a final decision arrived at concerning the use of the equipment for combined purposes.

3. Experience has demonstrated that the emergency issue of rotors by one country to the other is of considerable practical value and highly desirable. If the British machine were designed to use the same size rotors as those used in the CSP 1700, now held by the U.K. for submarine use, such emergency issue would be greatly facilitated. Therefore, the U. S. Chiefs of Staff recommend that the British Chiefs of Staff give consideration to this idea. Engineering drawings of the U. S. rotors will be provided on request.

TOP SECRET

~~TOP SECRET U. S. EYES ONLY~~

ENCLOSURE "B"

FACTS BEARING ON THE PROBLEM AND DISCUSSION

1. In RDC 5/99 dated 13 July 1949, the British Chiefs of Staff continued to express concern regarding the security of the present combined cipher machine on a long term basis and stated:

a. That they had decided to replace their main cipher machine (TYPEX) as soon as possible.

b. That they felt it necessary to have a single machine which would be able to provide both intra-British communications and combined U. S.-British communications.

c. That they requested the U. S. Chiefs of Staff to authorize the disclosure to the U. K. cryptographers of the principles and details of the ECM so that these might be incorporated in the new British machine.

2. In JCS 2074/2 dated 10 January 1950, the U. S. Chiefs of Staff denied the request but offered two alternatives:

A. The possibility of using a 7-rotor ECM.

B. As an alternative and as a possibly more rapid solution, it was suggested that the U. K. might wish to disclose either a copy of its new cipher machine, or detailed drawings thereof, so that the U. S. could ascertain the feasibility of constructing an adaptor for U. S. use which would provide the basis for secure combined communications by utilizing the new British machine, and an existing U. S. machine with an adaptor.

3. These alternative proposals will be examined in paragraphs 4 and 5.

4. Proposal A:

a. Development models of a 7-rotor ECM machine and also of a corresponding adapter to the ECM/SIGABA have been completed and their feasibility demonstrated. Assuming that service tests of this development proved satisfactory and mutually acceptable, this machine could be a long-term solution of the problem of highest level combined communications.

b. The security of the 7-rotor ECM is at least as great as that of the CSP 2900, the best machine the U. S. is now using. The 7-rotor ECM is therefore adequate for highest level combined communications.

~~TOP SECRET U. S. EYES ONLY~~

FACTS BEARING ON THE PROBLEM AND DISCUSSION (Continued)

g. The 7-rotor BCM can be adapted to work with our ECM/SIGABA, as well as with the present Combined Cipher Machine (CCM).

h. No additional information concerning the cryptographic structure of the ECM/SIGABA would have to be disclosed to the U. K.

i. Adoption of Proposal A would entail, so far as the U. S. is concerned, the development, testing, and procurement of a new machine for communicators who do not now hold the ECM/SIGABA, and also the development, testing, and procurement of an adaptor for the ECM/SIGABA. The estimated cost of development and procurement of these two equipments would be at least $6,000,000, which would have to be borne by the Services in proportion to the respective numbers of holders within each Service.

j. The time required for the foregoing development, testing, and procurement would be considerable. In addition a new procedure for the use of these new items would have to be developed and tested and personnel trained in their use, bearing in mind that the new procedure would necessarily be quite complex.

5. Proposal B:

a. The drawings of the new British cipher machine (Enclosure to JCS 2074/4 dated 13 April 1950) have been received and confirm the statement of the British Chiefs of Staff in Par. 6(b) of RDC 1/3 (Encl. A) JCS 2074/1, dated 6 December 1949, that the new British machine will operate on the broad principles of the ECM/SIGABA.

b. The British security evaluation of their new machine is sound; the resistance of the machine to cryptanalysis is at least as great as that of the CCM 2000. The new British machine will also be adequate for highest level communications.

c. It can be deduced from the drawings that the U. K. has not yet even built an engineering model of the new British machine, and therefore still has full latitude in the determination of certain details of basic construction.

d. Although the new British machine will embody the basic principles of the ECM/SIGABA, there are significant differences in detail. As a

~~TOP SECRET U. S. EYES ONLY~~

FACTS BEARING ON THE PROBLEM AND DISCUSSION (Continued)

consequence, in order to make the two machines intercommunicable, it would be necessary for the U. S. to provide the British with certain detailed information applicable specifically to the SCH/SIGABA. However, this would not include the complete details, some of which could be withheld permanently. Other details could be withheld until the British development had been completed and had been determined to be satisfactory by actual service test in combined communications.

g. The provision to the British of detailed information about the SCH/SIGABA is not necessary for, and has no bearing on, the use of their new machine for purely British intra-communication. Its use for Combined Communications can be effected without even requiring a special adaptor, thus more than meeting the British objection to having two separate equipments.

f. If the British are provided with such detailed information, the security of the resulting combined system would be of the same order as that of the SCH/SIGABA.

g. The sole disadvantage of Proposal B is that it would be necessary to provide the U. K. with the detailed information referred to in sub-paragraph f above.

h. As regards the effects on our own security, of the disclosure to the British of the detailed information referred to above, there would be no change whatever in the security evaluation of the SCH/SIGABA. That evaluation is predicated on enemy possession of the machine itself and relies for security solely on regularly changing keying information. The privacy of U. S. communications against cryptanalytic attack by any foreign power, including the British, would not be altered. There is unanimous agreement on this point among U. S. technicians even taking into account cryptanalytic progress to be expected in the foreseeable future.

i. If it is assumed that the British would include in their new machine appropriate wiring, which would not affect its suitability or security for intra-British communications, and if certain special rotors were used by them, then, so far as concerns the U. S., a relatively simple method of use of the SCH/SIGABA without a special adaptor, but involving

~~TOP SECRET U. S. EYES ONLY~~

~~TOP SECRET - U. S. EYES ONLY~~

FACTS BEARING ON THE PROBLEM AND DISCUSSION (Continued)

only one specially wired rotor per machine would permit intercommunication between the new British machine and the U. S. machine.

j. The cost to the U. S. of the adoption of Proposal 2 would be small, approximately $10 per machine. The total cost would not exceed $100,000. Moreover, the construction of a new machine for U. S. holders who do not now have the SIGABA would also not be necessary.

k. No new items of equipment would have to be developed, service tested and procured, present U. S. procedure in the use of the SIGABA could remain unchanged and therefore there would be no delays so far as the U. S. is concerned, in preparing for combined communications.

l. The action required by the U. K. in connection with the design and use of their machine would be relatively simple, practicable, and, it is believed, would meet with British acceptance.

4. Points applicable to both Proposals:

a. Although this paper pertains to U.S.-U.K. communications, it should be understood that any new Combined Cipher Machine agreed upon for U.S.-U.K. communications may also have to be made available for use by the British Dominions as well as by other allied foreign countries.

b. Certain U. S. machines (CSP 1700/SIGROD) presently being used for combined communication purposes will probably continue to be useful to the U. S. for other purposes for years to come—even though the U. S. and the U. K. replace them for combined U.S.-U.K. use.

c. A machine of improved security would have to be issued to those U. S. commands from whom the SIGABA was withdrawn in 1947.

d. The effect upon the communication intelligence interests of the U. S. either during the present "cold war" or during actual hostilities, would be the same. If used by a foreign country, either machine, for all practical purposes, would be unbreakable by the U. S. Thus, so far as concerns the continued effectiveness of the U. S. COMINT effort there is nothing to choose between the two proposals.

e. Experience has demonstrated that the emergency issue of rotors by one country to the other is of considerable practical value and highly desirable. Regardless of which proposal is adopted, if the British machine were designed to use the same size rotor as that used in the U. S. SIGABA, such emergency issue would be greatly facilitated.