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

~~TOP SECRET~~

~~U.S. EYES ONLY~~

DRAFT

This was draft first proposed by Cryptor Sec Panel of JCEC. After pressure from AFSA, it was replaced by another marked J/SC 66/4 13 Dec 49

REPORT BY THE JOINT COMMUNICATIONS-ELECTRONICS COMMITTEE

to the

JOINT CHIEFS OF STAFF

on

REPLACEMENT OF THE PRESENT COMBINED CIPHER MACHINE

THE PROBLEM

1. To comment and make recommendations on memorandum from the British Chiefs of Staff (RDC 1/36, dated 5 December 1949, enclosure to JCS 2074/1, dated 6 December 1949) on replacement of the present Combined Cipher Machine (CCM).

FACTS BEARING ON THE PROBLEM AND DISCUSSION

2. See Enclosure "B"

CONCLUSIONS

3. It is concluded that:

a. The best solution to the problem is the release to the United Kingdom of the principles of the current CCM.

b. That complete interchange of cryptographic principles should not be approved, but that a limited agreement should be proposed.

RECOMMENDATIONS

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

~~TOP SECRET~~

~~SECRET~~

~~ENCLOSURE "A"~~

~~DRAFT~~

DRAFT

~~MEMORANDUM FOR THE REPRESENTATIVES OF THE BRITISH CHIEFS OF STAFF~~

The U. S. Chiefs of Staff have considered the proposals made in MMC 1/36 of 5 December 1949 concerning the replacement of the present combined cipher machine (CCM). The two requests contained in paragraph 7 of MMC 1/36 are discussed herein in turn.

a. The U. S. Chiefs of Staff are now of the opinion that the present U.S. cipher machine, the M-134, should become the combined cipher machine, and make a counter proposal to that effect. The U. S. Chiefs of Staff are unable to accept any of the alternatives submitted in the Appendix to MMC 1/36, (paragraph 7). The principles of the present CCM are considered by U. S. technical experts to satisfy completely the security requirements for combined communications.

b. With regard to complete interchange of cryptographic principles on a reciprocal basis the U. S. Chiefs of Staff regret that they are still unable to accept such a proposal. The U. S. Chiefs of Staff recognize however that in certain fields such interchange is necessary. It is therefore proposed that interchange of cryptographic principles, on a reciprocal basis, be confined to the following fields of communications:

(1) Teleprinter systems for passage of intelligence
(2) Low echelon (Minor War Vessels) telegraphic systems
(3) Merchant Ships telegraphic systems
(4) Meterological systems both telegraphic and teleprinter.
(5) Facsimile systems.

~~TOP SECRET~~

~~FOR SIGNAL~~

~~U. S. EYES ONLY~~

ENCLOSURE "B"

FACTS BEARING ON THE PROBLEM AND DISCUSSION

1. The United Kingdom has rejected a proposal of the U. S. (Enclosure "A" to JCS 2074, dated 18 October 1949) to adopt the M.C.M. for combined use. The major reason for this rejection is expressed in terms of a reluctance to undertake any adaptation of the typex because that equipment is scheduled to be replaced in five (5) years time.

2. The Joint Communications-Electronics Committee (JCEC) has re-examined the problem, particularly centering its deliberations around paragraph 7 of the Appendix to JCS 2074/1 which raises three new possibilities for combined cipher communications, as follows:

a. The 7-rotor M.C.M.

b. The 7-rotor M.C.M.

c. Both the 7-rotor M.C.M. and the 7-rotor M.C.M. at different communication levels.

3. In discussing the problem in the light of the new facts presented, the JCEC has ruled out all three (3) of the possibilities listed in paragraph 2 above and of necessity has returned to the original proposal of the United Kingdom regarding release to them of the basic principles of the M.C.M. The JCEC agreed to the following statements of the advantages of the use of the M.C.M. in future combined communications:

a. The M.C.M. is immediately available for U.S. use, and without cost.

b. In the event of an emergency before the United Kingdom could be in sufficient production to supply their own needs, the U.S. could issue a limited number of M.C.M.'s, again without cost, for high command use.

c. The U.S. now has available for its own use cipher machines of greater security than the M.C.M. Furthermore, developments under way at the present time offer possibilities of additionally improving that security. Thus, issue of the M.C.M. would not be a matter of releasing the best U.S. machine to other nations.

4. The communications intelligence arguments previously advanced against the issue of the ECM are even more valid against any of the latest proposals of the United Kingdom. The 7-rotor ECM is at least as resistant to cryptographic analysis as is the present ECM, the 7-rotor ECM is more so. The U. S. Communications Intelligence's position would suffer less against the ECM than against these alternatives.

4. Disadvantages of acceptance of the proposals for a 7-rotor ECM or a 7-rotor ECM are as follows:

a. Neither is available.

b. Production costs for machines for U. S. use will be considerable and the time delay at least three (3) years before full scale use would be possible.

5. The second part of the United Kingdom's proposal to effect complete interchange of cryptographic principles in a reciprocal basis is still considered unacceptable. However, certain limited interchange is necessary and advisable. Specific items requiring exchange of principles are listed in paragraph 5 of the enclosure to JCS 2074/1.

6. This study has been coordinated with the Armed Forces Security Agency Council (AFSAC).