~~TOP SECRET~~

COPY

COPY NO. 12

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

J/SC 66/4

13 December 1949

JOINT COMMUNICATIONS-ELECTRONICS COMMITTEE

SECURITY AND CRYPTOGRAPHIC PANEL

REPLACEMENT OF THE PRESENT COMBINED CIPHER MACHINE

Note by the Secretary

1. The enclosure, a report of the Joint Security and Cryptographic Panel is forwarded to the Joint Coordinating Panel for consideration and is circulated to the members of the J/SC Panel for information.

W. R. JOY
Secretary, Joint Security
and Cryptographic Panel

This draft was submitted to JCEC, which practically discarded it + produced another draft for coordination with AFSAC

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

J/SC 66/4

COPY

~~TOP SECRET~~

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

COPY

DRAFT

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 the memorandum from the British Chiefs of Staff (RDC 1/36, dated 5 December 1949, enclosure to JCS 2074/1, dated 6 December 1949) on the 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. Complete interchange of cryptographic principles should not be approved without qualification, but that a limited agreement in certain fields should be proposed.

b. The U.K. should be invited to disclose the new British Cipher Machine to the U.S., as the basis of adaptation to a new Combined Cipher Machine which would link together the new British Cipher Machine and the appropriate U. S Cipher Machine.

c. The U. S should agree that attempts be made to develop a 7-rotor BCM as one of the possible replacements for the present CCM However no definite commitment should be made as to the adaptation of the 7-rotor BCM until the U.S. is satisfied with the development.

d. The British propsal of a 7-rotor ECM should not be accepted.

e. Combined U.S -U.K. communications should continue in the

present CCM until an emergency, or until such time as a new combined cipher machine is available and accepted. Such improvements as increasing the number of rotors to a set, frequent supersession of rotors and key lists, interchangeable cam contours, and any other feasible material improvements should be introduced.

f. The U. S. should assure the U.K. that, in the event of an emergency before the completion of the new combined cipher machine, the U. S. will furnish to the U. K. a limited number of U. S. cipher machines to meet immediate urgent needs of highest command communications.

RECOMMENDATIONS

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

- - - -

COPY TOP SECRET

TOP SECRET

ENCLOSURE "A"

D R A F T

MEMORANDUM FOR THE REPRESENTATIVES OF THE BRITISH CHIEFS OF STAFF

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

a. Which cipher mechanism should be employed on a long-term basis within the Combined Cipher Machine:

Should the British Chiefs of Staff care to disclose their new cipher machine as the basis of a possible new combined cipher machine, the U. S. Chiefs of Staff will be pleased to consider this machine for such adaptation of both the U. S and U. K. designs as may be feasible to provide intercommunication.

However the U. S. Chiefs of Staff consider that the 7-rotor BCM mechanism with appropriate stepping provides adequate long-term security for combined communications and therefore recommend that the British machine be completed with this in mind. This is desirable in order that in the event the U. S. 7-rotor BCM development becomes satisfactory this mechanism might be an alternative replacement for the present Combined Cipher Machine.

b. The 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 without qualification. However, the U. S. Chiefs of Staff recognize that, in certain fields, such interchange may be very profitable to both the U. S. and the U.K., and are agreeable to making this the subject of a conference in Washington.

2. The U. S. Chief of Staff are in agreement that the potential insecurity of the CCM can be reduced in part by additional rotors in the set and by the ultimate addition of interchangeable tires bearing the stepping control notches, and that every effort should be made in these directions until the successor machine to the CCM is available for combined communications.

In this connection, in the event of an emergency before the com

TOP SECRET

~~TOP SECRET~~

pletion of the new combined cipher machine, the U. S. Chiefs of Staff assure the British Chiefs of Staff that every effort will be made to provide the U.K. with a limited number of U. S. cipher machines to meet immediate urgent needs of highest command communications.

- - - -

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

ENCLOSURE "B"

FACTS BEARING ON THE PROBLEM AND DISCUSSION

1. The U.K. has, for various reasons, rejected a proposal of the U. S. (Enclosure "A" to JCS 2074, dated 18 October 1949) to adopt the 5-rotor BCM for combined use.

2. The 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 ECM

b. The 7-rotor BCM

c. Both the 7-rotor ECM and the 7-rotor BCM at different communication levels.

3. With regard to the proposal made in paragraph 2a above, that is, the 7-rotor ECM, there is no such machine now in existence. The U. S cannot afford, from an operational and economic viewpoint, to consider producing such a machine. To do so would entail a shift from the present NCM-CSP 2900 program to which the U.S. is firmly committed. In fact, the U. S. Navy will commence use of the CSP-2900 as of 1 July 1950; the Army and Air Force will commence using this machine as soon thereafter as their produdtion requirements are met.

4. With regard to the proposal made in paragraph 2b. above, i.e., the 7-rotor BCM, it is probably feasible, from both cryptographic and engineering standpoints to produce an adaptor to the NCM-CSP 2900 machine, which would permit 7-rotor BCM combined communications. However, in order to assure combined communications to all U. S. commands, it would be necessary for the U. S. to provide a separate 7-rotor BCM for use in sensitive or semi-sensitive areas because just as the U.S. does not in peace time expose the ECM in such areas neither should the U. S. expose the CSP-2900.

TOP SECRET
COPY

TOP SECRET
U.S. EYES ONLY

5. A 7-rotor BCM would provide vastly more secure combined communications than either the CCM or the present 5-rotor BCM. The 7-rotor BCM should have security comparable to that of the ECM. This point cannot be established definitely until all cryptographic details of the 7-rotor BCM have been determined and appropriate security studies have been conducted.

6. With regard to the proposal made in paragraph 2c. above, i.e., both the 7-rotor ECM and the 7-rotor BCM at different communication levels, this proposal must be discarded in view of the facts stated in paragraph 3 above.

7. a. The security evaluation of the 5-rotor BCM made in the Appendix to JCS 2074/1 is substantially correct, but it implies that the evaluation is also applicable to the present ECM. It is certain that the application of the proposed British attach to the ECM is very much more complex and difficult.

b. Although the U. S. security experts agree that the evaluation is substantially correct with regard to the present 5-rotor BCM, it should be noted that the solution is based on the assumption that the rotors are physically compromised. Considering the care and expense that are taken in produding, shipping, and accounting for cryptographic material, the routine acceptance of a presumption that the rotors for a cipher machine must always be considered compromised appears to be considerably beyond the normal limits of calculated risk. Indeed, if it must be assumed that the rotors are always compromised, then there is no valid reason for not assuming that the key-lists are also always compromised.

(1) Further, the presumption concerning the 25-letter "crib" assumed that the crib is correctly placed in cipher message, and all time estimates of the soltuion are based on this assumption. As a matter of fact, both the U. S. and U.K., use two special encryption techniques, bisection and variable

TOP SECRET

spacing, specifically designed to hinder crib-fitting; they are very effective for that purpose.

c. Increasing the number of rotors in a CCM or BCM set from 10 rotors to 20 rotors would increase the length of time a hundred fold.

d. The introduction of rotors with interchangeable cam contours, and more frequent supersession of rotors and key lists in conjunction with an increased number of rotors to a set can make the security of the present CCM acceptable for a considerable period of time (at least five years)

8. The second part of the U.K.'s proposal, to effect complete interchange of cryptographic principles on a reciprocal basis, is still considered unacceptable unless qualified. However, certain limited interchange may be profitable to the U.S particularly in the following communication fields:

a. non-literal

b. low echelon literal

c. meteorological

d. merchant ships

9. This study has been coordinated with the Armed Forces Security Agency Council (AFSA).

- - - -