AJ-14

CSGAS

SUBJECT: CCM Modification

TO: Chief of Naval Communications
Room 2724
Department of the Navy
Washington, D. C.

1. Reference is made to the statement, dated 29 October 1947, but only recently received from the Services Cypher Policy Committee of the LSIB Cypher Policy Board, subject: Modifications to Improve the Security of the Combined Cypher Machine (Inclosure 1).

2. In connection with Paragraph 12 of that document, in which the suggestion is that the U. S. again re-examine the question, the Army Security Agency proposes that an early meeting be held between Army and Navy representatives, with a view to deciding and agreeing upon a joint course of action in the matter.

3. If the foregoing proposal is agreeable to you, it is suggested that the meeting be held at Arlington Hall Station on a date which is mutually satisfactory and which can be arranged by telephone.

1 Incl
Document of Services
Cypher Policy Committee

HAROLD C. HAYES
Colonel, Signal Corps
Chief, Army Security Agency

JAN 23 1948

SIGNED AND SENT OUT

[redacted]





SIS 19 Jan 48

1cd 18

# TOP SECRET

SERVICES CYPHER POLICY COMMITTEE

S.C.P.C. Paper No.3

## MODIFICATIONS TO IMPROVE THE SECURITY OF THE COMBINED CYPHER MACHINE.

1. It is now generally agreed that there is a need for improving the security of the existing Combined Cypher Machine (C.C.M.). The British authorities cannot contemplate any modification which would fall outside the scope of the Typex with C.C.M. Adaptor; and it is thought that equally the U.S. authorities will certainly not consider any modification which would be impracticable on their ECM Adaptor or on the C.C.M. Mark II.

2. It is considered that the possible modifications can be divided into two general categories :

(a) Modification of the stepping sequence.

(b) Introduction of a plugboard.

3. With regard to (a), two proposals have been put forward by the U.S. authorities. These are :-

(i) The introduction of rotateable and interchangeable cam contours.

(ii) A complete re-arrangement of the law of progression according to which the drums advance.

The modification required by (i) is that the existing turnover notches cut in the fixed rim of the drum are machined off and replaced by a thin metal ring. This ring, which carries the turnover notches, can be fitted to the drum in any one of the 26 angular positions, and any one of a set of such rings can be fitted to any drum.

4. This modification is capable of being applied to both the U.S. and British versions of the C.C.M. It is understood that field trials are shortly to be carried out by the U.S. into the reliability and performance of such a device.

5. The proposal would unquestionably give considerably higher security to the C.C.M., but it would not eliminate the short cycle of the three centre drums which is the fundamental weakness of the machine. The security would still be below that of the British Typex Mk. 22, and also, it is believed, of the U.S. intra high-grade machine cypher.

6. The scheme mentioned in para. 3 (ii) is as follows :

Numbering the drums from left to right, drum 3 moves with each encypherment as hitherto. Drum 3 controls drum 4 and drums 3

/ and 4

and 4 combined control drum 1 on a cyclometric principle. Drum 1 controls drum 5 and drum 5 controls drum 2.

The effect of this alteration would be to destroy completely the short cycle of 338 on the 3 centre drums. This would be a most valuable improvement and no other type of modification would have this effect. It has the further advantage of removing the necessity for any restriction in the number and positioning of the turnover notches.

7. On the E.C.M. Adaptor, or C.C.M. Mark II, the activity of the turnover pawls which advance the drums is controlled by solenoids which are themselves controlled by relays. These relays are operated by small levers which "follow" the contours of the rim in which the turnover notches are cut. By rewiring the connections between the relays and the solenoids the modification 3 (ii) could be very simply effected. However, this is not the case with the C.C.M. Adaptor for Typex. In this machine the turnover pawls are controlled by a purely mechanical device which is entirely satisfactory in the case where one drum controls its neighbour. But the modification requires that, amongst other things, drum 1 should control drum 5 and this would be exceedingly difficult to effect with the existing mechanism. It is understood to be the opinion of the U.S. engineers that this modification would be practically impossible on the C.C.M. Adaptor.

8. If the modifications 3 (i) and 3 (ii) could both be carried out, the security of the machine would be very greatly increased, but might still be rather lower than the U.S. intra high-grade machine and the British Typex Mark 22.

9. It seems to us that, within the framework of the limitations imposed by the two types of C.C.M. Adaptors, the proposals 3 (i) and 3 (ii) exhaust all the reasonable possibilities for improving the stepping arrangements of the machine. The only other expedient which remains is the introduction of a plug-board on the output (cypher) side of the machine. In theory, this is no doubt perfectly possible on both the U.S. and the British version of the machine; it is thought that the U.S. authorities would be very reluctant to agree to its introduction

10. The additional security which a plugboard would afford is not overwhelmingly large. The reason for this is that the fundamental short cycle of the three centre drums is not thereby destroyed. Modification 3 (i) above coupled with the introduction of a plugboard would still leave the machine less secure than both Typex Mk. 22 and the U.S. intra high-grade machine.

11. We are led to the following conclusions:-

(a) The only modification we can envisage which is capable of raising the security of C.C.M. to the level of Typex Mk. 22 would be a complete re-arrangement of the law of progression of the machine.

(b) It is extremely doubtful if this would be a practical proposition for the British C.C.M. Adaptor.

(c) The additional security afforded by a plugboard would scarcely justify the trouble and expense which would be entailed.

(d) The best practical step is to accelerate the introduction of rotateable and interchangeable cam contours.

(e) Every effort should be made to reach agreement with the U.S. authorities in the design and production of a brand new cypher machine for combined purposes.

12. With reference to paragraph VII (b) of the agreed U.S. -British Memorandum "U.S. and British Collaboration on Combined Cypher Machine

/ Development",

Development", dated 4th March, 1947, it is suggested that the U.S. Authorities might again re-examine the question in the light of the above remarks. We fully admit that the only ideas which we can reasonably put forward for the improvement of the security are still inadequate but should be glad to know whether the U.S. authorities can better them. It must again be stressed however, that a major modification of the C.C.M. or the production of a new machine based on old principles could not be contemplated by the British.

Offices of the Cypher Policy Board,
10, Chesterfield Street, W.1.

29th October, 1947.