20 6/0148-14

File
F

COMBINED CIPHER MACHINE

Minutes of a Meeting Held 28 February 1947

PRESENT

| U. S. Navy | U. S. Army | U. K. |
|---|---|---|
| Capt. Smith, Chmn | Mr. Friedman | Col. Marr-Johnson |
| Capt. Safford | Dr. Kullback | Capt. Wilson |
| Cdr. Seiler | Dr. Sinkov | Mr. Pendered |
| Cdr. Hargreaves | Mr. Barlow | |

Captain Smith opened the meeting by reading the joint United States report prepared in connection with RM-26. (Inclosure 1) The reading of this paper was followed by a brief discussion of the United States position. Mr. Friedman expressed the appreciation of the United States members for the frankness and unqualified manner with which the British had submitted their ideas for consideration and added that he felt that nothing has contributed more to the continuance of amicable relations in the cryptographic coordination between the two countries. He pointed out as an addition to the joint paper that the advantage of unenciphered indicators is of definite importance. The United States services are considering simplified handling of indicator systems with particular emphasis on procedures which would be carried out independently of the cipher machines themselves. Captain Smith felt that the machine should be used for the generation of indicators rather than any auxiliary equipment. Mr. Friedman went on to state that there would be considerable difficulty in attempting to justify such an engineering development as the construction of RM-26 in view of the fact that the CCM is available in large numbers and that so much emphasis in United States planning is being placed on low echelon communications.

Captain Safford for Navy indicated that a similar need for low echelon development had been indicated in their service; in particular, a request had been received from the Marines for a new low echelon device. Though the Marines indicated satisfaction with the Hagelin, they had been advised that the security of the Hagelin was not considered sufficiently great, and in addition they would like a keyboard attachment to their cipher machine.

Captain Smith made the point that although the British are committed to the supersession of the Typex, the United States is not committed to a replacement program. He suggested the possibility of agreeing to a modification of the CCM that could be undertaken in our laboratories and expressed the hope that an acceptable degree of security could thus be achieved.

Captain Wilson in answer to these remarks made the following points with regard to the scrapping of the Typex. That the prime movers in that connection had been the security people. He said that the machine could be modified and improved up to the level of the improved CCM, but even that increase in security was considered insufficient. From a practical standpoint the machine had been found reliable. It had stood up under a tremendous amount of use and a woefully inadequate program of maintenance. It had carried all of the British raw traffic with the special advantage of being able to handle both upper and lower case characters.

The possibility was then discussed of a continued investigation of the RM-26 with a view toward making it intercommunicable with the CCM. The development could take the direction of providing for a special use of the machine. For example some combined communications were certainly needed to implement the existing authority for collaboration in signal intelligence. If the machine proved successful for such purposes, a Combined use could later be worked out, and that perhaps would tend towards the desirability of collaboration on Combined systems in general.

Captain Wilson indicated that continued investigation by the British would include the idea of providing teletype facilities as well as including a machine to work with the improved CCM. It was appreciated, however, that the question had to be presented to higher authorities for approval. Captain Smith raised the point that as yet the United States services have not received orders to proceed on a program of collaboration in the development of a Combined machine.

Mr. Friedman then indicated that a good starting point would be the establishment of a set of Combined rules for security. This led to a discussion of the differences between the regulations of the two nations. From the point of view of the United States, signal intelligence considerations weigh equally with security considerations. The British policy does not differ from this in peacetime, but in wartime the British tend to place more emphasis on operational security. The two attitudes require the striking of a balance. It was suggested at this point that the British might study in this connection the Navy publication RPS-4B and the corresponding Army publication AR 380-5 and draw up a set of rules which could be presented to the Combined Communications Board. The United States would similarly prepare a proposed set of rules.

At this point Captain Wilson stressed the fact that the security of the present CCM is unsatisfactory and that any major change contemplated would take time. Could we consider an immediate change to changeable cam contours?

Captain Smith indicated that arrangements are being made for a test of the improved CCM with changeable cam contours. Information in this connection will be available in about two months and a complete statement of the results will be provided to the British. A further point was made by Commander Seiler that developments are also underway on the provision of a special rotor wiring machine which will be ready before long and will greatly simplify the rewiring of rotors. Mr. Friedman suggested the consideration of increasing the number of rotors in a complement, but the Committee agreed that it was preferable to provide for more frequent change in the present set of ten rotors as a whole rather than add more rotors to the present complement with infrequent change.

Captain Wilson presented a statement of the cryptographic security requirements desired in a new CCM. Briefly stated they are:

1. Re-encipherment of messages to be possible without the need of paraphrasing.

2. Elimination of bisection, burying and padding.

3. System must be immune against cribs.

4. No changes of setting of variable elements to be required within a message.

5. Indicator system to be as simple as practicable.

6. To allow the plain language text to be distributed without paraphrasing.

Some discussion was entered into with regard to the needs of low echelon secure communications. Mention was made of the SG-41, and the Navy improvement of the Hagelin. There was also some discussion of the desirability of intercommunication between the low echelon device and the high echelon device. It was decided that decisions with regard to collaboration in low echelon developments should be deferred to a later date.