REF ID:A2436078

TOP SECRET

DRAFT

Unofficially & personally handed to me by Burton-Miller on 29 Nov 49 after conference in Adm. Stone's office. J

COMBINED BRITISH - U.S. CYPHER MACHINE

The Problem

To devise means whereby the present C.C.M. can be replaced by a Combined cypher machine which will provide the highest possible security for the next 20 years.

Facts bearing on the problem

2. (a). The British version of the C.C.M. consists of the Typex machine with the C.C.M. adaptor.

(b). The Typex machine is one of the British national cypher systems and is scheduled to be replaced within the next five years.

(c). The C.C.M. adaptor is of no value without the Typex machine.

(d). The new British cypher machine must incorporate the mechanism of the agreed new Combined cypher machine in order to meet the requirement of the Royal Navy that the smaller ships shall carry only one machine.

(e). The new British cypher machine must be effective for the next twenty years.

(f). The design of the new British cypher machine is at present held up pending a decision on what mechanism is to be employed for combined communications on a long term basis.

Offer by the U.S. Chiefs of Staff of the B.C.M. for Combined use.

3. The B.C.M. is a five drum machine. The drum turn-over mechanism shows a material improvement over the C.C.M. Both the B.C.M. and the Typex machines could be modified to accept the 5-drum B.C.M. mechanism.

Combined British - U.S. appreciation of the security of the 5-drum B.C.M.

4. <u>With present knowledge and techniques</u>, an electronic analytical machine could be built within the next three years to operate at a speed of 100,000 tests per second.

5. On the presumption that the cryptanalyst was in possesion of :-

(a) a set of the ten rotors

TOP SECRET

(b) a 25-letter "crib";

one such a machine could theoretically solve a setting of a 5-drum cypher maze with a ten drum set of rotors in about two years.

6. The practicability of such an attack would depend on:-

(a) The number of machines which could be made available,

(b) The extent to which the speed of operation of such a machine could be increased.

7. It is estimated that the first machine of this type would cost about $500,000 and that further machines would cost about $100,000 each. It is anticipated that considerable improvement in the speed of operation of a machine of this type would be possible within the next five years.

8. The 5-drum B.C.M. though offering a material improvement on C.C.M. will therefore theoretically not defeat this form of cryptanalytic attack in three years time.

9. The above appreciation applies to all 5-drum cypher mazes and not exclusively to B.C.M. However, a 7-drum cypher maze would defeat this form of attack.

British conclusions on suitability of B.C.M. for Combined Communications.

As a long term solution.

10. In view of the foregoing the British could not contemplate building a 5-drum B.C.M.

11. A 7-drum B.C.M. would be acceptable from the standpoint of security but would involve the incorporation in the new British cypher machine of additional mechanism.

As a short term solution.

12. Due to space limitations in the B.C.M., the U.S. cannot at present accommodate a 7-drum B.C.M. within the carcase of the B.C.M. They can only accommodate a 5-drum B.C.M. machanism. On the other hand, the U.S. have already built a 7-drum machanism for association with the Typex machine. A 7-drum B.C.M. machanism is therefore unlikely to be available for Combined Communications for several years.

13. It would take about two years before the 5-drum B.C.M. adaptor could be available. This being so with the arrival of the new British cypher machine, the 5-drum adaptor would be obsolete within three years of its introduction.

14. The British would therefore be extremely reluctant to build 5-drum B.C.M. adaptors as a short term solution.

CONCLUSION

15. It is agreed that nothing less than a 7-drum machine will offer adequate security for the next twenty years.

16. At the present time the British are planning to incorporate in the new British cypher machine a cypher mase of at least seven drums operating on the S.C.M. principle.

17. To provide a 7-drum Combined system would require modification to the U.S. S.C.M. but need not require any further modification to the new British cypher machine, if S.C.M. principles are employed.

18. It should be pointed out that in view of the material advance in cryptographic techniques, the British would prefer not to employ either the B.C.M. or the S.C.M. principles in the new British cypher machine. However, until discussion between British and U.S. on all cryptographic principles and theories is authorised with a view to arriving at an agreed new approach to the problem, the British are forced to retain a mechanism of this description if Combined working is to be possible and if they are to incorporate "British National" as well as "Combined" principles within one machine, which is a requirement of the Royal Navy. This requirement is not so pronounced in the Army and Air Force, who at present have techniques different from B.C.M. and S.C.M. in use or under construction, for both "on-line" and "off-line" cypher working.

RECOMMENDATION

19. In view of the material advances recently made in the science of cryptanalysis and cryptography, the most effective solution to this problem would be achieved by free interchange between the British and U.S. of all cryptographic techniques and theories, without necessarily disclosing which of these were to be employed for national cypher channels of either nation. This would enable the most profitable course in terms of security, efficiency and practicability to be determined. Failing this, both nations are tied to the S.C.M./B.C.M. principles for Combined Communications for the next twenty years.

20. If this exchange of information is not authorised, then in view of the fact that the design of the new British Cypher Machine is held up pending a decision on what system shall be employed for Combined use on a long term basis, a decision must be taken without delay on whether:-

(a) the 7-drum S.C.M.
(b) the 7-drum B.C.M.
(c) both (a) and (b) above

are to be employed for this purpose.