NATO UNCLASSIFIED

~~SECRET-NATO~~

COPY NO. 37

S.G. 7/40 (FINAL)

21 June 1951

STANDING GROUP

DECISION on S.G. 7/40

A Report by the Communications-Electronics Coordination Section

on

PROVISION OF A GENERAL HIGH GRADE CYPHER SYSTEM FOR NORTH ATLANTIC TREATY ORGANISATION POWERS

Note by the Secretaries

1. On 21 June 1951 the Standing Group approved the recommendation in paragraph 16, page 5. The Enclosure was transmitted to All Member Nations (Except Iceland), SHAPE, SACLANT (when formed), and Secretaries of all Regional Planning Groups of the North Atlantic Treaty Organisation. (SGM-980-51)

2. This decision now becomes a part of and shall be attached as the top sheet of S.G. 7/40.

C. H. DONNELLY
E. B. W. CARDIFF
P. L. de MONTJAMONT
Secretaries

NATO UNCLASSIFIED

[redacted]

Obsolete See Doc Dest memo #5 - 15 Feb 80

COPY NO. 37

S.G. 7/40

18 June 1951

Pages 1 - 11, incl.

REPORT BY THE COMMUNICATIONS ELECTRONICS COORDINATION SECTION

to the

STANDING GROUP

on

PROVISION OF A GENERAL HIGH GRADE CYPHER SYSTEM FOR NORTH ATLANTIC TREATY ORGANISATION POWERS

(CECS 15/2)

THE PROBLEM

1. To provide high grade cypher systems for general use by the Naval, Army and Air Force Commands down to Divisional H.Q. or equivalent level and by all war vessels of high security status of the North Atlantic Treaty Powers in the event of war or emergency.

FACTS BEARING ON THE PROBLEM

2. A machine cypher system - Typex Mark II with Simplex settings - has already been accepted for use by the NATO Nations at the Governmental, Supreme Command and Commanders in Chief level.

3. Although suitable for use in the planning stages to carry traffic between a number of fixed headquarters and ministries, the above system would be useless for general operational communications since its security depends upon the use of numerous two and multi-way Simplex settings held by the limited number of authorities concerned. The use of these settings cannot be extended to communications of the armed forces where a flexible system of inter-communications between a large number of holders is essential.

4. The Combined Cypher Machine (CCM) is at present used by the Australian, Canadian, New Zealand, U.K. and U.S. Armed Forces as part of a high grade cypher system where flexibility of inter-communications between a large number of holders is required.

5. The issue of the Combined Cypher Machine could be extended to all other NATO Nations.

6. The issue of CCM to NATO countries for "second level" communications would make it possible, by means of this one machine to provide communications between "first level" and "second level" on a "general" (i.e. daily changing) rotor arrangement.

7. Experience has shewn that if machine cypher systems are used it is desirable to have "back-up" systems for emergency use.

8. The Principal Staff Officers Committee, Western European Region (U.K., France, Belgium, Netherlands and Luxembourg) has recommended (in WR/MC(50)224) that the Standing Group approve an "Interim Naval Cryptographic Plan," which is summarized in paragraph 11 below. It is estimated in this paper that the interim naval solution can be implemented within one year.

9. The proposed "Interim Naval Cryptographic Plan" provides for:

a. Immediate revision of the Anglo-French Basic Cypher to bring it into line with current requirements, e.g., modernizing vocabulary, and inclusion of other NAT Powers' naval vessels and authorities.

b. Immediate reprinting of the Anglo-French Basic Cypher as revised, with sufficient copies for all North Atlantic Treaty Organisation naval authorities and ocean going warships.

c. Production of 6-way one-time pads so as to provide for many intercommunication groups of naval authorities and senior officers afloat.

d. Production of multiple one-time "OUT" pads which would enable principal naval shore authorities to communicate securely with allied warships at sea.

10. The Western European Region paper mentioned in paragraph 8 acknowledges that the interim plan proposed in paragraph 9 will NOT provide for secure communications in the following cases:

a. From a ship of one Nation to a ship of another Nation.

b. From a ship of one Nation to a shore authority of another Nation, except insofar as liaison teams with national cyphers may be provided at Headquarters of shore authorities.

The above-quoted Western European Region paper estimates that in spite of these two limitations about 80 per cent of the total requirements would be met by the Interim Naval Plan.

11. While no firm target dates for the implementation of a CCM system for the use of the Navies of the N.A.T.O. can be formulated until the overall requirements are known, it is considered that such a system could be implemented more quickly for all the Navies of the N.A.T.O. than could the proposed "Interim Naval Cryptographic Plan."

12. N.A.T.O. communications pose a complex language problem which will exist whatever cryptographic systems are adopted. The problem can be overcome by either

a. Interpreters in all cypher offices

or

b. The provision of a basic code book so compiled that a message encoded from an edition in one language can be decoded into another language by reference to the appropriate edition. The former cannot be regarded as a practical solution in the general case.

13. A bilingual Naval basic book in English and French containing figure groups is already available, but not in sufficient quantities to meet NATO needs. (At the lower levels it is probable that these two languages will not be sufficient to meet all requirements).

14. S.G. 7/18 of the 28th June 1950 (Regulations Governing the Handling and Use of Cryptographic Material provided for the use of the North Atlantic Treaty Organisation (implemented by SGM-201-50 of the 20th July 1950)) states in paragraph 4 f (2) that cryptographic machines will also be handled in accordance with special instructions applicable to the particular equipment.

A U.S./British Commonwealth policy for safeguarding the CCM has been laid down and it is essential that a similar policy be issued to cover the remaining N.A.T.O. Nations.

CONCLUSIONS

15. It is concluded that:-

a. High grade machine cypher systems for the Naval, Army and Air Force Commands, down to Divisional H.Q. or equivalent level, and for all NATO war vessels of high security status are required immediately for international and inter-service traffic and in some cases intra-service traffic.

b. The existing Combined Cypher Machine should be made available to all NATO Forces, subject to the regulations governing the handling and use of cryptographic material provided for the use of the North Atlantic Treaty Organisation (S.G. 7/18 of the 28th June 1950) and to the special policy contained in the Appendix * hereto.

c. "Back-up" systems for machine cypher systems should be provided for emergency use.

d. The CECS of the Standing Group, NATO, should take steps to determine the NATO requirements for CCMs, systems, rotors, key lists and associated documents.

e. While no better alternative interim arrangement than that proposed in paragraph 5 of the Annex to WR/MC(50) 224 can be offered immediately to the Navies of the Western European Region, it is considered that a CCM system can be implemented more quickly for all the N.A.T.O. Navies than a system based upon the extension of the Western European Region arrangements to the countries of other North Atlantic Treaty Regions.

*NOTE: The Appendix hereto has been classified CONFIDENTIAL.

f. A CCM system for N.A.T.O. Navies and for existing N.A.T.O. Army and Air Force formations in Europe should be accorded first priority in the implementation of an overall plan.

g. While the language problem is recognized, it does not affect the proposed use of the CCM and should not be allowed to interfere with the consideration of the CCM to meet an urgent need for "second-level" communications. Accordingly, a separate report on the subject of code books should be made by the CECS to the Standing Group.

RECOMMENDATIONS REGARDING IMPLEMENTATION

16. It is recommended that a memorandum substantially as in the Enclosure hereto be approved.

COORDINATION

17. No coordination is deemed necessary.

ENCLOSURE

DRAFT

MEMORANDUM FOR: All Member Nations (Except Iceland), SHAPE, SACLANT (when formed), and Secretaries of all Regional Planning Groups of the NATO

SUBJECT: Provision of a General High Grade Cypher System for North Atlantic Treaty Organization Powers.

1. On_____the Standing Group approved a Report which concluded that:-

a. High grade machine cypher systems for the Naval, Army and Air Force Commands, down to Divisional H.Q. or equivalent level, and for all NATO war vessels of high security status are required immediately for international and inter-service traffic and in some cases intra-service traffic.

b. The existing Combined Cypher Machine should be made available to all NATO Forces, subject to the regulations governing the handling and use of Cryptographic material provided for the use of the North Atlantic Treaty Organization (S.G. 7/18 of the 28th June 1950) and to the special policy contained in the Appendix* hereto.

c. "Back-up" systems for machine cypher systems should be provided for emergency use.

d. The CCCS of the Standing Group, NATO, should take steps todetermine the NATO requirements for CCMs, systems, rotors, key lists and associated documents.

e. While no better alternative interim arrangement than that proposed in paragraph 5 of the Annex to WR/MC(50) 224 can beoffered immediately to the Navies of the Western European Region, it is considered that a CCM system can be implemented morequickly for all the NATO Navies than a system based upon the extension of the Western European Regional arrangements to the countries of other North Atlantic Treaty Regions.

---

*NOTE: The Appendix hereto has been classified Confidential

f. A CCM system for NATO Navies and for existing NATO Army and Air Force formations in Europe should be accorded first priority in the implementation of an overall plan.

g. While the language problem is recognized, it does not affect the proposed use of the CCM and should not be allowed to interfere with the consideration of the CCM to meet an urgent need for "second level" communications. Accordingly, a separate report on the subject of code books should be made by the CECS to the Standing Group.

2. It is requested that All Member Nations will signify to the Standing Group their concurrence or otherwise to the above conclusions as soon as possible.

APPENDIX

GENERAL POLICY FOR SAFEGUARDING THE COMBINED CYPHER MACHINE SYSTEMS

INTRODUCTION

1. The nations which have been authorized the Combined Cypher Machine (CCM) Systems recognize the need for safeguarding these systems and all the component parts thereof. To permit the maximum utility consistent with good security practices, the following rules and definitions are set forth as the policy for safeguarding the CCM systems.

DEFINITIONS

2. The CCM systems consist of an appropriate cypher machine, together with the associated adaptors, rotors, key lists, operating and maintenace instructions, diagrams, and all electrical mechanical and cryptographic developments of the CCM and its component parts.

3. The following equipments may be used as the Combined Cypher Machine:

a. The CCM mark II, a machine cryptographically and mechanically complete in itself.

b. The CCM Mark III, an adaptor for use with the Typex Mark II machine.

RULES FOR SAFEGUARDING

4. Neither the CCM systems nor any of the component parts thereof will be placed ashore in any territory except where armed personnel of the nations authorized to use the specific systems in question are stationed in sufficient numbers to safeguard its physical security. It shall be the responsibility of the Theater (Area) Commander or the Service Head of a nation concerned to decide when the foregoing conditions have been met in each specific instance.

5. The CCM (and adaptor) is classified CONFIDENTIAL, but all its associated cryptographic aids are SECRET. For liaison purposes, the CCM system and all its component parts taken as a whole shall be regarded as SECRET and handled accordingly. Information concerning a CCM system and any of the component parts thereof may be disclosed to authorized personnel of the armed services of those nations authorized to use the specific system, and to any citizens of these nations under the control of the Armed Services, but only to the amount and degree necessary for the discharge of their official duties. Moreover, it shall be the duty of Commanding Officers and custodians to prevent the detailed viewing of the CCM systems by other than these authorized personnel.

6. The CCM shall not be installed in any aircraft for use therein.

7. Except as provided below, shipments of the CCM systems should always be split in time and carriers so that each of the four elements; (a) any one of the CCM machines, and adaptor, (b) the instructions manuals, (c) the key lists, and (d) the rotors is shipped separately. Similarly, two or more editions of the same series of key lists or two or more sets of rotors, one of which will supersede the other, should always be shipped separately. None of the four CCM elements ((a), (b), (c), (d) above), should be transported by air over or near enemy territory. A specific exception to the foregoing rules for shipment may be made by a Theater (Area) Commander or one of the Service Heads, as required by the abnormal circumstances prevailing.

8. A CCM system and the component parts thereof shall not be issued to nationals of countries other than those authorized to use the specific system, but may be issued to communications liaison officers of the armed services of the holding nations, detailed for service with the Armed Forces of other allied nations, if this is necessary for furthering the military operations of the nations authorized to use the specific system. In such a case, the Theater (Area) Commander or the appropriate

Service Head will be responsible for determining whether such issue is necessary. If such issue is considered necessary, the Theater (Area) Commander or the appropriate Service Head will:

a. Specify the appropriate CCM publications to be issued which will be of a class commensurate with the rank of the allied authority to which the communications liaison group is assigned.

b. Inform the appropriate allied authority that the CCM system is being supplied in order to provide a suitable high grade means of allied communication for operational cooperation.

c. Before authorizing issue, insure that the appropriate senior allied authority understands and agrees to the conditions under which the CCM system is being supplied and in particular that the communications liaison officer will be afforded all the necessary facilities for carrying out his duties and for preventing the CCM system's being subject to detailed viewing by other than authorized personnel. When the system is issued under such circumstances, it will be the responsibility of the communications liaison officer to insure that the foregoing conditions are met and to report immediately to his senior officer (the authorizing authority) if he is prevented by the allied authority with whom he is serving from carrying out his instructions.

MODIFICATION OF THIS POLICY

9. If at any time a nation considers it necessary to deviate in any way from this policy, that nation shall inform the other nations concerned of the facts and circumstances and of the proposed change in policy. Any change in policy shall be effected by agreement among all of the nations concerned prior to any action being taken under the proposed change.

10. In the event that any nation finds it feasible to adapt a National cypher machine to the CCM systems, the policy for safeguarding the CCM elements, (rotors, adaptors, and key lists) used in connection with that National Cypher Machine will conform to the policy expressed herein.