U.S.

~~TOP SECRET~~ COPY NO: 1

OK

LCS(53)/OR/R(4) (Final)
6th November, 1953.

UK/US COMMUNICATIONS SECURITY CONFERENCE 1953.

Report of the Operational Requirements Sub-Committee

to the

Executive Committee.

UK/US/NATO Operational Requirement for Off-Line Cryptosystems.

Section I - Off-Line Machines.

A. Replacement of the Combined Cypher Machine.

1. The Operational Requirements Sub-Committee considered the replacement of the existing Combined Cypher system in the light of the decisions reached at the 1951 and 1952 Conferences and the exchange of telegrams between the U.S. J.C.S. and the U.K.C.O.S. which has taken place since the last Conference.

2. The following factors were taken into account:

a. All U.K. and U.S. Services agree to adopt the ADONIS cryptosystems for Combined and NATO use as soon as suitable equipments are available.

b. The U.K. Services do not consider that the AFSAM 7 provides all the user facilities desirable in an off-line cypher machine but nevertheless, they are prepared to adopt it for Combined and NATO working until the U.K. replacement machine is available and provided that certain faults which were discovered in the AFSAM 7 during the user trials are remedied.

c. The U.S. Services agree to adopt the AFSAM 7 for Combined and NATO use provided that the deficiencies discovered during the user trials are remedied. Efforts to remedy these deficiencies are under way but if these are not successful, implementation of the programme may be delayed. To cover this eventuality a contract to develop another ADONIS equipment (AFSAM 47B) has been initiated.

d. All U.K. and U.S. Services agree that for higher echelon use there is a requirement for a machine embodying the ADONIS principle which will be capable of five unit code tape operation, both input and output.

e. The Committee noted that an AFSAM 7 production contract has been placed and that the output is presently approaching 400 equipments per month. It considered that the known deficiencies probably can be corrected by introducing design changes in the production line. As soon as the design of the machine is finalised, production can be stepped up to 600 per month and it is estimated that sufficient equipments will be available to meet the UK/US/NATO second level requirement by July 1956.

f. The contract calls for the production of spare parts concurrently with the production of main equipments and these spare parts normally will be issued at the same time as the equipments.

g. The UK/US agreed security estimate of the life of the ADONIS cryptoprinciple is at least 10 years from this date.

/3.

844

TOP SECRET

3. The Operational Requirements Sub-Committee recommend that:

a. ADONIS be adopted as the new cryptoprinciple for combined and NATO off-line use.

b. 1st July, 1956, be agreed as the implementation target date for replacing the present CCM with an ADONIS equipment regardless of the equipment which embodies the principle.

c. Provided the corrective action being taken is successful, the U.K. accept the AFSAM 7 with U.S.-provided rotors for usage during the period interim to the development and production of a national U.K. equipment capable of ADONIS operation.

d. Consideration be given to providing an equipment embodying the ADONIS cryptoprinciple and having facilities for five-unit tape operation, both input and output.

e. The above agreement supersede the 1950 BRUSA agreement to adopt the BRUTUS cryptoprinciple as the CCM replacement.

B. Third Level Requirement for a Power Operated Machine.

4. The Sub-Committee reviewed the requirements for a power operated off-line cypher machine for Third Level Combined and NATO use. It was agreed that:

a. There is a major requirement for a machine for Combined and NATO Naval Third Level use.

b. There is a small requirement for a machine for Combined and NATO Air Third Level use.

c. There is no requirement, at present, for a machine for Combined NATO Army Third Level use.

5. The Sub-Committee recommend:

a. That ultimately, the power operated equipment adopted for second level Combined and NATO use be adopted for third level Combined and NATO use.

b. That until such an equipment is available the current interim arrangements should continue in force.

C. Third Level Requirement for a Machine Requiring No External Power Supply.

6. The Sub-Committee reviewed the requirement for a machine requiring no external power supply for Combined and NATO use at the Third Level. The U.S. Services restated their view that a machine requiring the use of dry batteries, such as PORTEX, is unsuitable for such a purpose; the U.K. Services stated that they would be prepared to use such a machine.

7. It was agreed that:-

a. There is a requirement for a small machine requiring no external power supply for use at the Third Level when international forces are employed in the Assault Phase of an operation.

/b.

TOP SECRET

b. There is no equipment presently available which will meet this requirement but the D.17 appears to provide a possible ultimate answer to this problem.

8. The Sub-Committee recommend:

a. That selection of an equipment requiring no external power for Combined and NATO use at the Third Level be deferred.

b. That, in the interim period, since they are likely to be the major parties in any international assault group, the U.K. and U.S. should accept responsibility for providing to such NATO elements as may be co-operating with them such cryptographic equipment as may be available at the time.

Section II - Third Level Hand Systems.

A. NATEX.

9. The Operational Requirements Sub-Committee re-affirmed the decision of the 1952 Conference that NATEX is required:-

a. At the Second Level as a back up to CCM owing to the shortage of machines.

b. As an interim low echelon cryptosystem.

10. The Sub-Committee agreed that although theoretically, and in conformity with the above policy, there should be a NATEX key for COSMIC traffic as a back-up for the CCM COSMIC key list (AMSP 294), the preparation of such a key was not justifiable since all posts requiring to handle COSMIC traffic were equipped with CCM most of them having more than one machine.

Keys Required.

11. The Sub-Committee agreed that the following NATEX keys are required for NATO use:-

a. Peace Time

(1) Three Services World Wide (ACPs 270/2)

(2) Small Ships World Wide (AMSPs 273/5)*

(3) Classroom Training (AMSPs 288/290)

b. War Time

(1) Naval General Area 1 (AMSPs 279/281)

(2) Naval General Area 2 (AMSPs 282/284)

(3) Small Ships Area 1 (AMSPs 273/5)*

(4) Small Ships Area 2 (AMSPs 276/8)*

* Note: There will be no Small Ships World Wide key in war.

/Definition

Definition of Areas.

12. The Sub-Committee agreed:

that it was desirable that areas should be provisionally agreed to enable correct quantities to be estimated and to facilitate stockpiling of war reserves at overseas distributing authorities and that cryptographic areas should conform to Operational areas.

Use of NATEX with Basic Book.

13. The Sub-Committee took note of the Security Committee's statement that, if used with a basic book, the security of NATEX would be considerably improved. There would be the following advantages -

a. longer messages could be sent without change of indicator

b. higher traffic loads could be permitted

c. variable spacing need not be used

d. the basic book might be expected to condense the length of the encrypted text.

14. The Sub-Committee accordingly agreed that the U.K. should carry out trials using a basic book with NATEX to determine its practicability, bearing in mind particularly the possibility of an increased number of garbles and greater difficulty in solving them.

Simplified Indicator Procedure for Third Level Use.

15. The Sub-Committee took note that, at the request of Belgium, the U.S. had prepared a simplified NATEX indicator procedure for intra-national low echelon use.

16. The Sub-Committee agreed that the U.K. should study the new procedure from an operational standpoint and report on its possible use for Combined and NATO third level communications.

B. Transport Aircraft Code.

17. The Sub-Committee took note that in accordance with the agreement reached at the 1952 Conference that there is a Combined UK/US and NATO requirement for a Transport Aircraft Code, the problem had been considered by the CAN/UK/US J.C.E.Cs and a draft code prepared. Since this draft code was not yet available for study in the Air Ministry no further progress on this item was possible at this time.

C. Aircraft Movement Code.

18. The Sub-Committee took note that the requirement for an Aircraft Movement Code had recently been referred by the CAN/UK/US J.C.E.Cs. to the Air Standardization Co-ordinating Committee for compilation of the information required to be included in aircraft movement pro-formas.

19. The Sub-Committee agreed -

a. that when the aircraft movement pro-formas were available it would be necessary to consider a code of combat type for encoding them for use when the aircraft movement messages could not be encrypted on standard on-line or off-line cryptosystems available on the communication circuits concerned.

/b.

b. that, in order that preparation of the necessary crypto systems may begin, the urgent need for the provision of aircraft movement pro-formas should be represented to the A.S.C.C. through the J.C.-E.Cs.

D. Maritime and Maritime Aircraft Code.

20. The Sub-Committee took note that the main requirement for a Maritime and Maritime Aircraft Code for tactical inter-communication between ships and aircraft had been met and the necessary publications were in course of production.

21. The Sub-Committee however agreed -

a. that there was a requirement for Maritime and Maritime Aircraft Code to be used in routine exercises in peace time since this traffic might reveal information on A/S warfare techniques to a potential enemy;

b. that G.C.H.Q. should complete their examination of routine exercise traffic already sent in by the Admiralty and Air Ministry;

c. that as a result of this examination G.C.H.Q. should recommend a suitable rate of change for an edition used world wide for routine exercises in peace time;

d. that in the interim period before this edition was available, increased security for this traffic could in many cases be provided by a more rapid change of the U.K. Maritime Aircraft Reporting Code, and that action should be taken to effect this;

e. that the practicability of using ACP 176 recoded instead of Maritime and Maritime Aircraft Code should be examined by U.K. and U.S.

22. The Sub-Committee confirmed that there was an operational requirement for Maritime and Maritime Aircraft Code to be carried by Carrier-borne aircraft in air strikes over enemy territory, and that there was therefore a big risk of physical compromise.

23. The Sub-Committee therefore agreed -

a. that Maritime and Maritime Aircraft Code was unsuitable for passing to and from maritime aircraft information of long term intelligence value;

b. that there was a requirement for a rapid and secure system suitable for this purpose;

c. that the suitability of AFSAM 7 for this purpose should be investigated by the U.K. and U.S.

e. Bomber Code.

24. The Sub-Committee took note that the main requirement for Strategic and Theatre Bomber Codes had been met and that the necessary publications were in course of production.

25. The Sub-Committee however agreed -

a. that there was a requirement for Bomber Code to be used in routine exercises in peace time since this traffic might reveal information of value to a potential enemy;

/b.

b. that the U.K. and U.S. should examine the requirement in detail to determine the number of editions required and the rate of change of editions necessary if adequate security was to be provided.

F. Naval Tactical Codes.

26. The Sub-Committee reviewed the requirement for naval tactical codes. Representatives of the Royal Navy and U.S. Navy propounded the respective merits of a book system, such as Fleet Code, and of a high grade machine cryptosystem.

27. The Sub-Committee took note -

a. that ciphony would be the ultimate answer to a large part of the problem;

b. that for CW -

(1) the Royal Navy considered that the requirement could best be met by a book system such as Fleet Code possibly revised and made a good deal smaller;

(2) the U.S. Navy considered that the requirement could best be met by a high grade machine cryptosystem and that security considerations demanded such a system.

28. The Sub-Committee agreed -

a. that the Royal Navy should re-examine the use of a high grade machine cypher with a view to its eventually meeting the CW requirement;

b. that both the Royal Navy and U.S. Navy should consider the requirement for a tactical code, small enough to enable the code to be changed daily, for UK/US and NATO use in the interim period until a suitable machine cryptosystem and ciphony are available.

Section III - Submarine Communications.

A. Normal Duty.

29. The Sub-Committee agreed -

a. that for normal duty submarines should carry the machine cryptosystem in general use for second level communications;

b. that so long as LUCIFER remains in use separate rotors and key lists should be provided for use by submarines;

c. that when ADONIS replaces LUCIFER it will no longer be necessary for submarines to carry special rotors, but special key lists will still be required.

B. Hazardous Duty.

30. The Sub-Committee agreed -

a. that for hazardous duty, submarines should carry the machine cryptosystem in general use for second level communications using normal duty rotors as in paragraph 29 above;

b. that special hazardous duty submarine key lists should be provided;

c. that submarines should destroy normal duty key lists before entering hazardous waters.

/c.

C. Back-up System.

31. The Sub-Committee agreed -

a. that there was a requirement for a secure hand back-up system;

b. that trials should be carried out using a specially prepared basic book with garble-free letter groups recyphered by letter one-time pad;

c. that the basic book should be prepared by N.S.A. in conjunction with the U.S. Navy;

d. that since the basic book will be used only with one-time pads it can be compiled as a one part book (i.e. having combined code and decode);

e. that copies of the basic book should be supplied to the U.K. to enable trials of the system to be carried out concurrently in the Royal Navy and U.S. Navy.

D. Change from LUCIFER to ADONIS.

32. The Sub-Committee took note that, since submarines can carry only one machine, it would be necessary to bear this fact in mind when the time came to change from LUCIFER to ADONIS for submarine communications.

Section IV - Weather Security

33. The Sub-Committee wished to record that in the past weather communications security requirements have too frequently been considered as different from and handled differently from operational communications security requirements. This separation was illogical and often led to weather requirements being overlooked in the compilation of general crypto-requirements. Because of the long time required to finance and manufacture crypto equipment, failure to include all requirements at the proper time could mean failure to provide essential security.

34. The Sub-Committee therefore recommended that in the future weather communications security requirements should be incorporated as part of the complete operational communications security requirement for crypto equipment.

Section V - Merchant Ship Communications.

A. Merchant Ships Cryptosystem.

35. The Sub-Committee agreed -

a. that, since no machine system and no better hand system than MERSEX was available for general and convoy merchant ship communications, MERSEX should continue to be used for these purposes;

b. that, as a general guide, the merchant ships cryptosystem (MERSEX) should be held by merchant ships of 500 tons gross or over fitted with W/T.

/36.

36. The Sub-Committee took note that U.S. proposals for a new cryptosystem designed to replace the MERSEX Independent Keys would be put forward shortly and would be considered by the U.K. in due course.

B. Cryptosystem for Merchant Ship Control Traffic.

37. The Sub-Committee agreed that there was no way of meeting the communications security requirement for Merchant Ship Control Traffic unless Chapter 5 of ATP 2 was much modified. It was however understood that U.S. proposals to amend this chapter were to be expected shortly, and that these proposals were designed greatly to decrease the volume of signalling by each NCSO. Until these amendments were agreed no action to plan the cryptosystems required for this traffic could be taken.

38. The Sub-Committee however considered that a machine cryptosystem was probably required at the larger ports, but that traffic originated at the minor ports could be carried by hand systems; possible systems were one-time pad or NATEX.

C. Other Merchant Ship Traffic.

39. The Sub-Committee took note of the requirement to encrypt a large volume of traffic originated by shipping companies and their agents and that this would probably be encrypted partly by naval and partly by censorship authorities.