CONSEIL DE L'ATLANTIQUE NORD
NORTH ATLANTIC COUNCIL

249

EXEMPLAIRE N°
COPY

~~SECRET~~ CONFIDENTIAL

ORIGINAL: ENGLISH
22nd February, 1965

NATO ~~SECRET~~
DOCUMENT
~~MBC-M(65)65~~
AC/4-D/1764

Jan. 5/3/65 incorporated

INFRASTRUCTURE COMMITTEE AND MILITARY BUDGET COMMITTEE

TROL CRYPTOGRAPHIC EQUIPMENT PROCUREMENT PROGRAM

Memorandum by Chairman of the Military Budget Committee and Acting Chairman of the Infrastructure Committee

Council has instructed the Infrastructure and Military Budget Committees jointly to determine how a program for procurement of tapeless, rotorless on-line(TROL) teletypewriter cryptographic machines for NATO Commands should be financed (C-R(64)20 approving Enclosure 2 to MC 74-1 as amended by C-M(64)11(Revised)). The purpose of this memorandum, which has been seen and agreed by SHAPE, is to give details of the nature of the program and to point out the financing problems that will have to be considered and resolved.

General

2. In line with general Council policy on communications security, the Supreme Allied Commanders are proposing to re-equip NATO telegraph circuits with TROL crypto machines.

3. Standing Group, Major NATO Commanders and nations have endorsed a policy of total encryptation of all communications. The procurement program now being put forward proposes TROL crypto machines for every telegraph circuit in NATO commands required for peace and war. It is envisaged that NATO nations will install compatible equipment.

4. It is being proposed for Allied Command Europe that international funds be used to provide equipment for national ends of NATO circuits at the next level below international headquarters.

The Procurement Program

5. Equipment that will meet the military requirement has recently become available. In competition, four such machines have been evaluated and one proposed for procurement. The projected program for procurement and installation is as follows:

Phase I - Planning and contracting in 1965

Phase II - Production and installation from 1966 into 1968

Phase III- Consolidation and complete use starting in 1968. It is expected that the equipment will be in use until about 1978.

6. SHAPE will be sole contracting agent for ACE and its Communications Security Organization will exercise management control. SHAPE is willing to act as procuring agent for other Supreme Commands and will probably be asked to do so.

Size and Cost of the Program

7. On the basis of equipping all its telegraphic circuits, both permanent and reserve, SHAPE places the ACE requirement at 1,473 duplex and 663 simplex machines for a total of 3,609 units. The requirements of SACLANT and CINCHAN, already programmed in the Slice XIII Infrastructure, are 295 and 56 units, respectively. (Two units would be required for each duplex and one unit for each simplex circuit).

8. The estimated cost of a duplex unit is £7,000, and of a simplex unit £5,000. On this basis, the ACE financial requirement is placed at:

1,473 duplex units at £7,000	£10,311,000
663 simplex units at £5,000	3,315,000
Total	£13,626,000

In assessing the total cost of the ACE program, SHAPE has added 10 per cent each for transportation (the machines would have to be moved by courier), installation and contingencies, and 5 per cent for training. This would amount to £4,769,100, to bring the total cost to £18,395,100.

9. The SACLANT request in the Infrastructure program is for £576,000 and the CINCHAN request for £116,400, these being for machines only. These are now know to be far too low. A re-pricing would indicate a maximum order of magnitude of:

(a) For SACLANT - For equipment, £1,475,000 to £1,525,000; for transportation, etc., £515,000 to £535,000, a total of £1,990,000 to £2,055,000.

(b) For CINCHAN - For equipment, £285,000; for transportation, etc.; £100,000; a total of £385,000.

Since SACLANT and CINCHAN have presumably provided for their requirements on the basis of indicating units rather than simplex and duplex machines, a reworking of their requests to provide for simplex and duplex machines should give firmer estimates than those quoted above.

10. The indications nevertheless are that the total NATO program as envisaged by Supreme Commands will be somewhat in excess of £15,000,000 for machines and £5,000,000 for the follow-on expenditures.

Production and Installation of Equipment

11. It is estimated that with a large order, such as the approximately 4,000 units foreseen for NATO, a monthly delivery rate of 150 simplex or 75 duplex equipments could be attained 12 months after receipt of order. On volume production, the NATO order could be produced in about 27 months. The elapsed time from ordering to completion of contract would be approximately three years, which is the proposed project time mentioned in paragraph 5.

12. Since encrypted messages cannot be sent over a circuit until crypto equipment is installed at the sending and receiving ends, communication experts say that it is not reasonably possible to lay down an installation program that caters to a priority, such as equipping strike force circuits before others or a segment of the system before the rest. If this was done, very little of the system would become operational until a high proportion of the machines were installed. To get progressive implementation, machines will have to be installed circuit by circuit between two communication centres, followed by another two centres. While it is possible to exercise some judgment as to which centres will be hooked together before others, the real determining factors of the sequence will be such things as importance of message traffic, location of currently-used crypto equipment, state of implementation of TARE, etc.

13. For the above reason, it is not necessary to think of phasing the delivery of equipment on a year-by-year basis to complete segments of the overall system. In other words, from the installation point of view, a three-year program is not more advantageous than a five-year program. Supreme Commanders opt for the three-year program for reasons of security - to improve security and extend it to the entire system as quickly as possible.

14. Comparative details of the operating and technical characteristics of TROL crypto machines and the one-time tape on-line machines now in use is given in the Annex.

Financing

15. As already noted, SACLANT and CINCHAN have had their request for TROL crypto machines logged with Infrastructure for several years.

16. SHAPE, in bringing forward the ACE requirements, has tentatively suggested a breakdown of financing of 75 per cent for the Military Budget Committee and 25 per cent for Infrastructure Committee. The basis of the breakdown is past experience in allocating requirements of peace headquarters to the Military Budget Committee and those of war headquarters to Infrastructure Committee. With the policy of the last few years of having all communications located in the war headquarters when it becomes operational, it becomes difficult to draw a precise distinction between peacetime and wartime use of the facilities of the military communications system. It is therefore hard to justify a 75-25 split or any other proportionate division based on a peace-war criterion.

17. If one prefers a definable basis for allocating financing between the two Committees, the most readily available and probably the most easily justified is to make the Military Budget Committee responsible for equipping the permanent circuits and Infrastructure Committee the reserved circuits. Another formula would be to make Infrastructure Committee responsible for financing the machines and the Military Budget Committee responsible for transportation, installation and training costs and those contingency costs not directly associated with the machines themselves.

18. The truth of the matter, however, is that there is no recognised criterion for allocating financing between the two Committees for a project such as this, and the final decision must possess a substantial measure of arbitrariness. Since the project will probably involve one procurement agent, it would make considerable sense to allocate financial control, regardless of source of funds, to one committee only. The obvious nominee is the Infrastructure Committee because of its experience in and resources for handling large contracts. In this case, it might be considered desirable for this Committee to assume the financing as well, since the follow-up maintenance and operating costs will be a Military Budget Committee responsibility. Alternatively, Infrastructure Committee could exercise financial control over the project, and the source of funds could be pro-rated between the two Committees on an agreed basis, such as 75-25, 60-40, etc.

19. An arbitrary allocation could be 50-50, on the ground that it would equalise the "burden-bearing" of all countries arising from differential cost shares under the Infrastructure and Military budget cost-sharing formulae.

Conclusions

20. The Infrastructure and Military Budget Committees are requested jointly to determine the basis of financing of a program for equipping the telegraphic circuits of NATO Commands with tapeless, rotorless, on-line cryptographic machines. To this end, they should determine:

(a) Whether all or only a part of the telegraphic circuits will be terminated with TROL machines. The Working Group of National Communications Experts can advise on this matter. It would also seem desirable, at an appropriate time, for this Group to screen carefully the permanent and reserve telegraphic circuits to fix the number of TROL equipments that will be ordered.

(b) Whether TROL machines will be installed at international charge at national terminals of NATO circuits one echelon below NATO Headquarters, as was done on a loan basis for one-time tape, on-line crypto machines now being used in ACE.

(c) Over how many years the procurement program will be phased.

(d) What elements of cost - machines, transportation, installation, training, etc. - will be considered an integral part of the project for special financing, and what parts the normal costs of operating a headquarters and therefore financed under the Military budget.

(e) How the procurement and installation program costs will be allocated between the Infrastructure and Military budgets.

(f) Whether one or both Committees will participate in the financial management of the procurement and installation programs, and, if shared, the division of responsibility between them.

(Signed) M. CHASE
Acting Chairman
Infrastructure Committee

(Signed) A.S. DUNCAN
Chairman
Military Budget Committee

OTAN/NATO,
Paris, XVIe.

TECHNICAL AND OPERATING INFORMATION ON EXISTING AND PROPOSED ON-LINE TELETYPE CRYPTOGRAPHIC EQUIPMENT

At the present time, ACE has 1,239 on-line cryptographic machines, divided 639 ETCRRM, 180 ETCRRM Modified, and 420 ECOLEX. The holdings of other Supreme Commanders are not known but will be substantially less than those of ACE.

2. Both the ETCRRM and ECOLEX originate from a common cryptosystem conceived prior to World War II. The ETCRRM is an earlier model and has been in use in NATO for five to ten years, while ECOLEX has been in use for about two years.

3. Having a common origin, the two machines have similar performance characteristics. They are on-line rotor equipments using one-time tapes. Both equipments transmit material slowly, are expensive in terms of operator-maintenance time and in the consumption of one-time tape and spare parts. They require extensive separation from associated equipment and line units and must be housed in an operation centre with a clear zone of about 200 metres in order to avoid unacceptable radiation. It has also been found necessary to install power-line filters in each communication centre. Although the cost is not yet known, each centre will need as many as six filters at a cost of about F. 5,000 each.

4. More serious than the operational limitations of the machines are their limitations in terms of security. It was found that the ETCRRM radiates its impulses with the result that with the right kind of equipment and conditions it was possible to intercept its message traffic. As a consequence, the machines cannot be used for messages classified above Confidential. With a supression modification carried out in 1964, some of the machines can now carry messages up to Secret. ECOLEX has greater overall security. It is also capable of traffic flow security, i.e., of transmission of an uninterrupted flow of random text with no indication of what part comprises encrypted message text. However, if so used, it is estimated that the 420 ECOLEX machines in ACE would consume F. 25,000,000 of one-time tape per year. However, the ECOLEX is subject to a component failure at unpredictable times that will result in it passing information to the line in clear. The correction of this fault is costing about F. 173,000.

5. Neither equipment will operate with telegraphic automatic relay equipment (TARE), except on a fully attended basis, so no saving of personnel, operating costs or circuits can be realised. This will become an increasingly important consideration, since TARE is becoming operational in AFSOUTH, is being installed in AFCENT, and is being programmed in the Slice XVI Infrastructure for NORTHAG/2ATAF and CENTAG/4ATAF.

6. SHAPE considers the two types of equipment as obsolescent from the point of view of performance and security. The ECOLEX, modified to improve its security, has a somewhat further useful life. However, with the introduction of TARE, both equipments, in modified or unmodified forms, can be considered obsolete.

7. The equipment recently proposed for NATO use is based on a different principle of encryptation than the ETCRRM and ECOLEX, and therefore has few of their operating characteristics. It does not, however, involve new technology, and is expected to be highly reliable in operation and relatively inexpensive to maintain. The equipment is built up of components, so local maintenance should seldom involve more than component replacement. For ACE, SHAPE is proposing to centralise higher echelon maintenance under its control. Since the machines use low-level keying, the elaborate radiation shielding precautions need for currently-used crypto machines is unnecessary.

8. Security will be high with the new equipment. The machine has traffic flow security at modest extra cost. Traffic flow security is enhanced by the fact that "set, check, and receipting" will no longer have to be done by plain language contacts. Furthermore, where off-line encryptation is now needed for a variety of messages due to the relatively low security of the machines in use, it will only be needed when the new machines are in use for messages requiring exceptional safeguards. (SHAPE reports that off-line encryptation in preference to on-line encryptation is not yet acceptable because high-speed off-line devices have not been developed, would involve the use of ancillary terminal equipment and would reduce traffic flow security).

9. The present on-line machines must be located alongside the telegraphic equipments they are serving. As a result, both equipments must be together in a traffic hall and be attended, on an individual position basis, by an operator trained for both teletype and crypto equipment, and therefore fairly skilled. The new machines can be remotely located from the telegraph equipment. The communication between the two centres need to be only a signal system to indicate circuit readiness. Where the communication centre is large enough, crypto operators and teletype operators instead of crypto-teletype operators can be used. The crypto operator can handle 12 crypto machines and the teletype operator about five teletype machines, where the crypto-teletype operator can handle only one combined equipment at a time. The teletype operator need no longer be skilled since his principal task will be inserting and removing teletype tapes. The new machines, therefore, are labour-saving. Another labour-saving feature is that where traffic must be manually logged and receipt with current crypto machines, this will be done automatically with the new machines.

10. The new machines are capable of operating with all current and projected teleprinters. This includes high speed teleprinters, since the machine has a speed from 45.5 to 750 bauds against 45.5 and 50 bauds for the existing equipments. Finally, the equipment can be used with TARE. When so used, messages will have to be deciphered at each switching centre and enciphered for onward transmission because of technological difficulties with the cryptographic and communication systems. This can only be cured when broad band encryptation becomes possible. This is not, however, a serious weakness since the changes cipher-clear-cipher will be done automatically.