~~CONFIDENTIAL-NATO~~

COPY NO. 24

S.G. 7/22

22 September 1950

STANDING GROUP

DECISION ON S.G. 7/22

A Report by the Communications Electronics Coordination Section

on

SUPPLEMENTARY INFORMATION REGARDING THE DISTRIBUTION OF TYPEX/SIMPLES PADS

1. On 20 September 1950, the Standing Group approved the recommendations contained in S.G. 7/22, paragraph 5, page 2.

2. The memorandum was transmitted to all Military Representatives Accredited to the Standing Group and Secretaries, Regional Planning Groups on 20 September 1950 (SGM-346-50).

3. This decision now becomes a part of and shall be attached as top sheet of S.G. 7/22.

C. H. DONNELLY
E. B. W. CARDIFF
R. A. VALLET
Secretaries

~~CONFIDENTIAL-NATO~~
Dec. on S.G. 7/22

Obsolete
See Doc Dest memo #5
15 Feb 54

~~CONFIDENTIAL NATO~~ COPY NO. 24

S.G. 7/22

24 August 1950

Pages 1 - 5 incl:

REPORT BY THE COMMUNICATIONS ELECTRONICS

COORDINATION SECTION

to the

STANDING GROUP

on

SUPPLEMENTARY INFORMATION REGARDING THE DISTRIBUTION OF TYPEX/SIMPLEX PADS.

THE PROBLEM

1. To disseminate information regarding the distribution of Typex/Simplex Pads to users of the Typex cryptographic system within the North Atlantic Treaty Organisation.

FACTS AFFECTING THE PROBLEM

2. Details of the plan for the provision of crypto channels for North Atlantic Treaty Organisation communications during the planning stage using Typex II and Simplex Settings have been promulgated. (SGM-200-50 dated 20 July, 1950) and equipment is now being issued.

3. Instructions for the operation of Typex II are also being issued; these, however, do not elaborate the arrangements being made for the distribution of Typex/Simplex Pads. This was explained verbally to cypher operator trainees at the various courses, now completed, in London and Washington.

CONCLUSION

4. It is concluded that the appended supplementary information regarding the distribution of Typex/Simplex Pads should be transmitted to all users of the Typex cryptographic system within the North Atlantic Treaty Organisation.

RECOMMENDATION

5. It is recommended that a memorandum substantially as attached at the Enclosure hereto be approved.

COORDINATION

6. No coordination is deemed necessary.

E N C L O S U R E

D R A F T

MEMORANDUM FOR ALL MILITARY REPRESENTATIVES ACCREDITED TO THE STANDING GROUP AND SECRETARIES, REGIONAL PLANNING GROUPS.

SUBJECT: Plan for the provision of crypto channels for North Atlantic Treaty Organisation communications during the planning stage using Typex II and Simplex Settings - Supplementary information regarding the distribution of Typex/Simplex Pads.

REFERENCE: SGM-200-50 dated 20 July, 1950.

On _____, the Standing Group approved a Report by the Communications Electronics Coordination Section which concluded that the appended supplementary information regarding the distribution of Typex/Simplex Pads should be transmitted to all users of the Typex Cryptographic System within the North Atlantic Treaty Organisation.

A P P E N D I X

DISTRIBUTION OF TYPEX/SIMPLEX PADS

1. In their simplest form, the Simplex Pads consist of two copies - the "TWO", one OUT copy and one IN copy. This enables A, the holder of the OUT copy, to send a message to B, who holds the IN copy. For B to send a message to A, it is necessary for B to hold an OUT copy of an entirely different "TWO" and A must hold the IN copy of it. To avoid mistakes, the names of the holders of the OUT and IN copies must be clearly written on the covers of the pads before they are despatched to the holders.

2. In addition, where necessary, "multiple" series of pads are provided, enabling the holder of the OUT copy to send the same cryptogram to a number of addresses. The title indicates the number of copies of the pad; of these copies only one is marked OUT; the remainder are all IN pads, e.g.

A "THREE" means A holds the OUT pad and there are two IN copies held by B and C.

A "SIX" means A holds the OUT pad and there are five IN copies held by B, C, D, E and F.

The pads constituting a complete network enabling all holders to communicate with one another, are known as a "set"; e.g. a set of "THREES" comprises 3 editions - 9 pads in all - held as follows:-

A holds say No. 105 OUT
B and C hold No. 105 IN
B holds say No. 106 OUT
A and C hold No. 106 IN
C holds say No. 107 OUT
A and B hold No. 107 IN

3. A central office (e.g. a Secretariat) which requires to send out circular telegrams, may therefore hold, say, a "FIFTEEN" OUT pad for sending a telegram to fourteen addresses, each of which holds a copy marked "FIFTEEN" IN.

4. A "FIFTEEN" OUT should never be used for a message to a single address to which a "TWO" is available, nor for a message to, say, three addresses to which, say, a "FIVE" OUT is available. However, it is sometimes a convenience to use a pad such as a "FIFTEEN" OUT for a multiple address to, say, ten of the holders of the IN copies, rather than encrypting the message more than once, using different OUT pads. When certain messages are not addressed to all holders, the addressees omitted will find that they receive subsequent messages using indicators beyond the indicator which they have marked as the last one used.

5. It may be found occasionally that it is required to send a telegram to an address for which no OUT pad is held. In this event, it will be necessary to route the telegram through a third office (e.g. a Secretariat) for which an OUT pad is held and which is known to hold an OUT pad to the ultimate addressee; this intermediate office would decrypt the telegram and re-encrypt the plain language, using the appropriate OUT pad to the final address. (Forwarding instructions must be encrypted in the first encryption).

6. When the first issues of pads are made to holders more than one "edition" may be provided. One edition may be reserved for messages of the highest secrecy (possibly bearing a special codeword) which may only be handled by specially nominated cypher operators; another edition would then be provided for messages of lower classification. In addition, there may be a third edition to be held as a reserve to replace the current edition when that has been used up or in the event of compromise of the current edition. For the latter reason, the reserve edition should, if possible, be stored, in another safe, apart from the current one. In every case the purpose of each edition should be clearly marked on the cover of the pad.

7. WARNING. As laid down in the Typex Operating Instructions (NAT/01/1)* an OUT pad must be used for encrypting messages; IN-pads may only be used for decrypting messages received.

* Copies of these Instructions will shortly be issued.