

~~SECRET~~
~~SECURITY INFORMATION~~

20


USCIB: 29.1/2

30 September 1953

~~SECRET - SECURITY INFORMATION - U.S. EYES ONLY~~MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Disclosure of the ADONIS (US) Cryptoprinciple to NATO Countries.

1. The enclosure is circulated for the information of members at the suggestion of the Director, National Security Agency.
2. The enclosure is considered of interest in connection with security problems involving third parties to BRUSA.


RUFUS L. TAYLOR
Captain, U.S. Navy
Executive Secretary, USCIB

Enclosure

NSA ser 00752 dtd 26 SEP 1953.

REPRODUCTION OF THIS DOCUMENT IN WHOLE
OR PART IS PROHIBITED EXCEPT WITH
PERMISSION OF THE ISSUING OFFICE.

USCIB: 29.1/2

~~SECRET~~

~~SECRET~~~~SECURITY INFORMATION~~NATIONAL SECURITY AGENCY
WASHINGTON 25, D. C.

Serial: 00752

26 SEP 1953

~~SECRET - SECURITY INFORMATION~~MEMORANDUM FOR THE CHAIRMAN, STATE-DEFENSE MILITARY INFORMATION CONTROL
COMMITTEE

SUBJECT: Disclosure of the ADONIS Cryptoprinciple to NATO Countries

1. The problem of secure communications for North Atlantic Treaty Organization (NATO) military forces has been considered in a series of annual conferences on communication security matters between the U.S. and the U.K. Existing cryptographic systems available for NATO use are inadequate. Except for NATO Confidential and Restricted, all NATO classified messages may be encrypted only in systems authorized by the Standing Group. The only authorized systems now are:

a. One-time pads. This system is not feasible for widespread use.

b. One-time tape equipment. This system is not feasible for widespread use and there is an inadequate supply of equipment.

c. The British Typex/Simplex. This system is limited in the same way as one-time pads and by an inadequate supply of machines.

d. The Combined Cipher Machine.

e. The French modified M-209 for low-echelon use.

2. The Combined Cipher Machine (CCM) is being used among second level NATO commands only. There are not enough machines for distribution to lower levels. Furthermore, the CCM is considered by U.S. and U.K. experts to offer less security than desired and should be replaced as soon as suitable equipments become available.

3. The U.S. Joint Chiefs of Staff and the British Chiefs of Staff have considered the matter of replacement of the CCM and both have approved joint Conference recommendations that the machine selected to replace the CCM be also used as the NATO machine.

4. The cryptoprinciple favored by the U.S. Joint Chiefs of Staff for replacement of the CCM is the ADONIS cryptoprinciple as embodied in the AFSAM-7 and the AFSAM-47B. The ADONIS crypto unit consists of an

Enclosure with USCIB 29.1/2 dated 30 September 1953.

~~SECRET~~

~~SECRET~~~~SECURITY INFORMATION~~~~SECRET - SECURITY INFORMATION~~Serial: 00752
26 SEP 1953

eight-rotor non-reciprocal permuting maze. The rotors have 36 contact points and are constructed with rotatable and interchangeable alphabet and notch rings. The notch rings govern the stepping of the rotors during operation. Ten output contact points of the maze are permanently connected to ten input contact points as re-entry circuits thus confining the cipher output to 26 letters. The ADONIS cryptoprinciple is considered by both U.S. and U.K. cryptographic experts to afford adequate security for the purpose intended, and that its disclosure will not endanger U.S. communication security.

5. It is requested that the State-Defense Military Information Control Committee approve the release of the ADONIS cryptoprinciple to the NATO nations for the purpose of meeting NATO military communication security requirements.

(Signed)

RALPH J. CANINE

Lieutenant General, US Army
Director

Copy furnished:

Executive Secretary, USCIB

~~SECRET~~