CONFIDENTIAL - NATO COPY NO. 15

NORTH ATLANTIC MILITARY COMMITTEE

COMITE MILITAIRE DE L'ATLANTIQUE NORD

Standing Group Groupe Permanent

SGM-634-53

14 April 1953

MEMORANDUM FOR ALL MEMBERS NATIONS (Except Iceland)
SACEUR
SACLANT
Allied CINCCHANNEL
EMCCC
ACCA

SUBJECT: Interim Instructions for NATO Users on Categories of Cryptosystems and on Multiple Encryptions

1. NATEX and French modified M-209 cryptosystems are vulnerable to cryptanalytic attack if the unaltered plain texts of messages encrypted therein become available to unauthorized persons. These cryptosystems are called Category B. All other NATO cryptosystems are called Category A. To protect Category B cryptosystems from cryptanalysis, the plain texts of messages encrypted in those systems must be paraphrased whenever those texts received dissemination which might permit them to fall into unauthorized hands. The circumstances under which paraphrase is required are as follows:

a. If a message is to be encrypted in a Category B cryptosystem, it must first be paraphrased if it has had unclassified dissemination, if it was received from sources outside a national Service authority, if it was previously encrypted in any system, or if it has been transmitted in the clear over any circuit except an approved circuit laid in a military reservation or on board ship or where the possibility of undetected interception is negligible.

b. When a Category B message is received, it must be paraphrased before being reencrypted in another Category B

DIST: A D E1 F G1, 2, 3 H2 X: ACCA - 10 Cys

cryptosystem. If it is reencrypted in a Category A cryp system, no paraphrase is required but the abbreviation "BECAT" must be inserted immediately following the security classification in the text of the reencryption to indicate to the receiving cryptocenter that the message must be handled as Category B despite receipt in a Category A cryptosystem.

c. Texts which have been encrypted in a Category B cryptosystem or which contained the abbreviation "BECAT" require paraphrase prior to their dissemination in any manner which might permit exposure to unauthorized persons. Therefore, paraphrase of Category B messages is required before they may be declassified or disseminated outside a national Service authority. For the same reason, they must be paraphrased prior to their clear transmission over any circuit except an approved circuit laid in a military reservation or on board ship or where the possibility of undetected interception is negligible.

2. The following rules always apply when:-

a. Any message, or part thereof, is encrypted in more than one cryptosystem because all of the addressees do not hold a cryptosystem in common, or

b. any message, or any of the plain text thereof, having once been encrypted and transmitted, has subsequently to be encrypted by the originating headquarters or by one or more of the addressees.

(1) A different message (or starting point) indicator shall be selected for each encryption.

(2) When procedures such as bisection and variable spacing are required, the manner of their application shall be varied in each encryption.

(3) When more than one encryption is made the same date-time group must not be used for each encryption.

Therefore, for the second and any additional encryption, the original date-time group (if it must be transmitted for reference purposes) must be encrypted in the text as part of the codress. The date-time group of the second and any additional encryption will be deleted from decrypted copies, the original date-time group being reinserted if necessary.

(4) There shall be no external linkage between the encryptions, or between the original message and the reencryption.

3. The foregoing procedure will become effective without further notice on 1 May or as soon thereafter as possible.

FOR THE STANDING GROUP:

M. de Chabot

M. de CHABOT
Lt Colonel, Fr Army
Deputy Secretary