

USCIB: 29.1/7

16 December 1953

~~TOP SECRET~~

MEMORANDUM FOR THE MEMBERS OF USCIB:

Subject: Program to Improve the Communications Security of
NATO Countries.

Reference: USCIB 29.1/6, dated 15 December 1953.

1. Enclosed is a corrected page 2 of enclosure 7 with the reference.
2. Please substitute this page for the one contained in the reference and destroy the replaced page.


H. D. JONES

Deputy Executive Secretary, USCIB

Enclosure
a/s

USCIB: 29.1/7

~~TOP SECRET SECURITY INFORMATION~~

III. NON-ADDITIVE HAND SYSTEMS

6. There are many hand systems of encipherment that do not employ additive. Very few of these can be guaranteed to be secure, even though they may be very complex, applying both substitution and transposition to code or plain language.

IV. MACHINE SYSTEMS

7. Machine ciphers vary greatly in the amount of security they afford. Failure to observe in every detail proper instructions for operation may lead to compromise even with the best machines. Others, such as the well-known Hagelin "Cryptoteknik" (see para 8 below) are insecure unless precautions are taken over and above those recommended by the manufacturer. Others, again, are basically insecure and should in no circumstances be used.

8. Special attention is drawn to the dangers inherent in the use of the Hagelin "Cryptoteknik" machines of the C-series:

a. Since the encipherment is essentially by additive, it follows that if a message setting is used more than once the key can be recovered on the overlap; a single mistake by an operator using a message setting a second time can thus compromise the machine setting.

b. The additive generated by the machine is never truly random and there are circumstances in which this fact can be used to recover the machine setting, even though no message setting is repeated.

c. With proper precautions this machine can give very good security for a limited amount of traffic, but in view of the number of different dangers that can arise in varying conditions of use, for which it is impossible to legislate in advance, member nations who wish to make use of the "Cryptoteknik" are especially urged to consult SECAN.