~~SECRET - SECURITY INFORMATION~~ 25 November 1953

DRAFT MEMORANDUM FOR STANDING GROUP TO ISSUE

1. Regulations at present in force (DC 2/7 (Final) and STAND 474 as amended by STASECS 1508, 1535 and 1588) ensure that all COSMIC telegrams and all NATO TOP SECRET and SECRET telegrams are encyphered in cryptosystems authorized by the Standing Group. But all nations of NATO are also originating and transmitting in their own national cryptosystems a quantity of telegrams both civil and military which, although they are the private concern of the nation in question, must be expected to contain information which affects NATO as a whole and the loss of which to a non-NATO nation harms the security of NATO.

2. Further STAND 474 allows NATO telegrams graded CONFIDENTIAL OR RESTRICTED to be encrypted in national systems, and it is highly undesirable that information of such gradings should become available to nations outside NATO.

3. The Standing Group therefore feels considerable concern at the potential danger to the security of NATO which may arise from the insecurity of the national communications of individual nations: the insecurity of one can endanger the security of all.

4. The Standing Group has had prepared a paper enumerating examples of cryptographic and communications practices and procedures which endanger security. This paper is attached at Appendix A. The Standing Group requests that each member nation examine this paper and take action to ensure that its own communications are free from the practices and procedures mentioned therein.

5. Further the Standing Group requests that each NATO nation will designate or establish a Communications Security Agency which shall be authorized to communicate on communication security matters both civil and military direct with the Standing Group Communications Security and Evaluation Agency Washington (SECAN) and with the European Security and Evaluation Agency (EUSEC).

6. The Standing Group invites any member nation, which requires advice and technical assistance towards the improvement of the security of its national cryptographic and communications practices and procedures whether civil or military to apply through their Communications Security Agency direct to the Standing Group Communications Security and Evaluation Agency Washington. It may subsequently be found more convenient for SECAN to arrange for discussions arising out of this first approach to be held with EUSEC.

DRAFT

~~TOP SECRET - SECURITY INFORMATION~~ 25 November 1953

LIST OF EXAMPLES OF DANGEROUS CRYPTOGRAPHIC AND COMMUNICATIONS PRACTICES AND PROCEDURES

I. UNENCIPHERED CODES.

1. Unenciphered codes are totally inacceptable in diplomatic use for transmission of classified information. They are only acceptable for Armed Forces communications when it is not considered essential to maintain the security of the information for more than two or three days from the introduction of the code. It follows that such codes must be changed at very frequent intervals.

II. ADDITIVE SYSTEMS

2. Any additive (or subtractor or minuend) system is dangerous unless special precautions are taken in the construction of the additive itself. Many procedures that may be regarded as "special precautions" are deceptive as to security and may even in themselves create weaknesses.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

[redacted]

5. In general, polyalphabetic substitution systems whether actually additive in nature or not, are like additive systems and are subject to the same dangers.

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

~~TOP SECRET~~ CONTROL NUMBER 53-41-231
4 20 — COPIES
PAGE 1 OF 2 PAGES

"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.

V. TRANSMISSION SECURITY.

9. Ciphers, however good individually, are not enough to ensure communications security. Transmission techniques and message formats can in themselves provide considerable intelligence to a traffic analyst. Although there are practical limitations, the ideal to be striven for is that the traffic neither of any type (e.g., naval, air force, etc.) nor of any nation should be distinguishable by external characteristics. Again, intelligence can be gained by study of the organization and procedure of radio networks and by use of radio direction-finding. In many cases, especially in Armed Forces communications, a skillful enemy can obtain valuable intelligence by collation of apparently uninformative message texts. It follows, therefore, that full communications security demands that special precautions be observed in such matters as the judicious employment of indicators, the selection of call signs and of frequencies, radio procedures, and the restriction of the use of plain language.

~~TOP SECRET~~ CONTROL NUMBER 53-41-231
COPY 4 OF 20 ~~PAGES~~ COPIES
PAGE 2 OF 2 PAGES