

~~SECRET~~COPY

24 March 1944

MEMORANDUM FOR Security Section

I. The following information was gathered through discussion with Colonel Fahnestock, Chief, G-2 Classified Message Center, Major Battin of Special Branch, G-2, and Lt. Forbes, Security Officer, War Department Code Center, in regard to a memo from G-2 dated 11 March 1944, Subject: Handling and Distribution of Messages Concerning Combined Subjects.

1. That 51 copies of messages in the TAM-MAT series are made by War Department Classified Message Center as listed in Annex 2, this memo. Similar distribution is given to the CAL-LAC, GOV-VOG, LEM-MGL, NAF-FAN, FACS-SCAF, MEG-GEM, and BOC-COB series. Only in one instance is paraphrase attempted despite regulations in AR 380-5 cited in Annex 1. Messages to the State Department are sometimes paraphrased although the original copy is usually seen by the State Department before paraphrase is attempted.

2. Thirteen copies of the original messages are given to the British without paraphrase. The British distribution is not exactly known although undoubtedly original copies wind up in the British Embassy, the British Message Center, British Chiefs of Staff and the British War Office. Therefore, although some attempt is made to paraphrase messages sent to our own State Department, the British Embassy and War Office are furnished with the original version. It is also believed that a copy of the original message reaches the British inner sanctum where it is available for cryptanalytic study.

3. Most of the traffic sent in the TAM-MAT, etc. series has been in SIGABA. The SIGABA has always been regarded as the backbone of cryptographic communication in both the U. S. Army and U. S. Navy and therefore the utmost enforcement of physical and cryptographic security has always been afforded this equipment. Regulations have been issued forbidding the showing or discussion of SIGABA with the representatives of any nation but our own. However, from the above information it appears that, for an undetermined time, the British have been given the opportunity for unlimited exploit of the SIGABA from a cryptanalytical point of view.

4. All of the traffic to War Department in the TAM-MAT etc. series is sent through regular War Department channels and must clear through either London or Algiers. Both London and Algiers are now equipped with and are now using one time tape systems. Therefore, it would be an easy matter to route all traffic in the TAM-MAT etc series over SIGTOT channels. This would eliminate the need for paraphrase in any case and would also

COPY

~~SECRET~~

~~SECRET~~

COPY

save the SIGABA from further exposure.

II Recommendations:

1. That a directive be issued by G-2 stating that all traffic in the TAM-MAT etc series be transmitted only in SIGTOT.
2. That an effort be made to restrict similar traffic where distribution of unparaphrased messages is made to a government other than the U. S. or to another agency in our government to one-time systems.
3. That an investigation of the practices referred to above be instigated and that every effort be made to enforce the security regulations. On the face of it, this looks like one of the most serious threats to the security of our cryptographic systems that has yet come to light.

William A. Henning Jr.
1st Lt., Signal Corps

COPY

~~SECRET~~