

DRAFT

~~TOP SECRET~~

12 May 1945

SUBJECT:

THRU: Assistant Chief of Staff, G-2, and
The Chief Signal Officer

TO: Commanding General, Army Service Forces

1. The following information relative to United States, German, and Japanese signal security equipment is furnished for inclusion in reply to memorandum from General Marshall to General Somervell dated 3 May 1945.

2. Speech Security Equipment:

- a. U. S. Army -- RC-220-⁻¹~~TX~~ High security equipment for transoceanic telephonic communication on Staff and High Command levels.
- b. German Army and Air Force -- No comparable item known.
- c. Japanese Army and Air Force -- No comparable item known.
- d. Evaluation:
 - (1) RC-220 ⁻¹~~TX~~. No known method of solution; no indication of cryptanalytic study or successful attack by enemy.
 - (2) The Japanese have used low-security speech equipments to a limited extent. All forms have been solved by U. S. Army technicians.

~~TOP SECRET~~

3. Teletype Security Equipment:

a. U. S. Army -- Converter M-228 and SIGTOT equipments. The former is a medium security, the latter a high security mechanism for automatically enciphering and deciphering teletypewriter signals, permitting handling of large volumes of traffic by wire and radio.

b. German Army and Air Force -- "Geheimschreiber" equipment. Similar in function to Converter M-228.

c. Japanese Army and Air Force -- No comparable item known.

d. Evaluation:

(1) SIGTOT equipment: No known method of solution; no indication of cryptanalytic study or successful attack by enemy.

(2) Converter M-228 equipment: Methods of solution applicable under certain conditions are known; no indication of cryptanalytic study or successful attack by enemy.

(3) Geheimschreiber: Methods of solution have been evolved, applied successfully, and a large amount of traffic solved by British, with U. S. Army cooperation and assistance. Exceptionally valuable intelligence obtained from all high-echelon channels on which it was used.

4. Cryptographic Equipment.

a. U. S. Army

~~TOP SECRET~~

- (1) Converter M-134-G: A keyboard operated, printing cipher machine capable of enciphering messages of all classifications at the rate of fifty (50) words per minute. Widely distributed to all large fixed headquarters and to headquarters of tactical units down to and including division headquarters.
- (2) Converter M-209: A small, manually operated, mechanical printing cipher machine for low-echelon tactical communications.

b. German Army and Air Force: "Enigma" cipher machine. A keyboard operated, non-printing cipher machine with maximum speed of operation limited to approximately five (5) words per minutes.

c. Japanese Army and Air Force: No comparable equipment known to be in use although recent information indicates that there is one under development. These organizations now use very cumbersome "paper and pencil" hand methods.

d. Evaluation:

- (1) Converter M-134-G: No known method of solution; indications of cryptanalytic attack by German, with no success whatever.
- (2) Converter M-209: Methods of attack under certain conditions are known; indications of cryptanalytic attack by Germans and Japanese, with limited amount of success, due to improper use of the device by certain units lacking

~~TOP SECRET~~

~~TOP SECRET~~

adequate training and supervision.

- (3) "Enigma" cipher machine: Employed to encipher highest level administrative and command traffic. Methods of solution have been evolved and applied successfully by British with considerable assistance and cooperation from U. S. Army. A large volume of intelligence of highest importance obtained from the successful reading of this traffic.
- (4) Japanese cryptographic systems: Methods for their solution have been evolved and applied successfully by the U. S. Army with the resultant production of a large volume of important intelligence.

~~TOP SECRET~~