SECRET

SECURITY IMPROVEMENTS ACCOMPLISHED BY "C" BRANCH IN 1944

Following is a summary of activities designed to improve the security of communications in the U. S. Army during 1944.

1. PROCEDURES FOR INCREASING CRYPTOGRAPHIC SECURITY.
   a. Introduction of new cryptographic systems.
      (1) Literal one-time pads.
      (2) Aircraft warning service cipher.
      (3) Radio direction finding cipher.
      (4) AACS PX codes.
      (5) Authentication Systems 3, 4, 5.
   b. Modification in method of channel elimination for strip systems.
2. PROCEDURES FOR INCREASING PHYSICAL SECURITY.
   a. Establishment of new clearance procedure.
   b. Compilation of file of cryptographic custodians.
   c. Promulgation of rules in document form.
3. PROCEDURES FOR INCREASING TRANSMISSION SECURITY.
   a. Expansion of monitoring control and missions.
   b. Standardization of monthly report form.
   c. Distribution of dissemination charts, reports, etc.
   d. Preparation of scripts of training records.
4. NEW DEVICES AND MACHINES PLACED IN SERVICE.
   a. Speech equipment AN/GSQ-1( ).
   b. Converter M-325.
   c. Converter M-218( )/U.
5. NEW OR IMPROVED MACHINES IN DEVELOPMENT.
   a. Converter M-294.
   b. Converter M-409.
   c. Speech equipment AN/GSQ-2.
   d. Facsimile equipment AN/GXA-2( ).
   e. Converter attachment AN/GSA-2.
   f. RADCO device.
6. MODIFICATIONS OR IMPROVEMENTS IN EXISTING MACHINES.
   a. Modified Converter M-228.
   b. Equipment for one-time tapes.
   c. Redesigned parts for Converter M 134-C and Converter M-228.
7. ESTABLISHMENT OF NEW CRYPTONETS.
   a. Cryptonet 37 (POA and SWPA using Converter M-228).
   b. Cryptonet 38 (Worldwide AACS using Converter M-228).
   c. Cryptonet 39 (20th Air Force).
   d. Cryptonet 40 (Joint Army-Navy).
   e. Cryptonet 41 (Persian Gulf Command).
   f. Cryptonets 97, 98, and 99 (Training cryptonets).
8. IMPROVEMENTS IN CRYPTONETS.
   a. Inclusion of necessary types of systems.
   b. Discontinuance of certain systems.
9. IMPROVEMENTS IN LIAISON.
   a. Within Army.
      (1) Decentralization of accounting, making theaters suboffices of record.
      (2) Assistance given theaters in production of material.

COPY

SECRET

b. With Navy.
   (1) Exchange of holder lists.
   (2) Establishment of joint Army-Navy cryptonet.
   (3) Preparation of one-time tapes for Navy.

c. Combined operations.
   (1) Publication of combined documents.
      (a) Field code.
      (b) Instructions for air-ground authentication system.
   (2) Policy permitting use of Converter M-228.

10. IMPROVEMENTS IN OPERATIONAL PROCEDURES.
   a. Utilization of "G" Branch facilities for producing cryptographic material.
   b. Formation of lay-out room for multilith stencils.
   c. New checking procedures.
   d. Addition of new equipment for printing of material.

11. SECURITY STUDIES.
   a. Determination of security limits of cipher machines and devices.
   b. Analysis of traffic cryptographed in various systems to determine weaknesses.
   c. Transmission security analysis of tactical monitoring logs.
   d. Study of procedure for reporting compromises and cryptographic violations.
   e. Study of call signs, system indicators, and internal references.
   f. Study of necessity for paraphrasing cryptographed messages which are also transmitted in plain text over classified circuits.

12. NEW OR REVISED PUBLICATIONS.
   a. Systems instructions.
   b. AG and SPSIC letters.
   c. Monthly Informational Document.
   d. Articles and posters in Signal Corps Technical Information Letter.

The following discussion amplifies certain points found in the above outline. Main paragraph headings below are numbered to conform to those of the outline.

1. PROCEDURES FOR INCREASING CRYPTOGRAPHIC SECURITY.

a.

a. Aircraft warning service cipher, radio direction finding cipher, and AACS PX codes were prepared for use by the Air Forces.

b. Authorization was granted for three specific authentication systems for intra-Army and joint Army-Navy use.

c. The new method of channel elimination for strip systems provides a high degree of security by requiring that both the particular channels eliminated and the total number of channels eliminated will vary among messages enciphered on the same day.

2. PROCEDURES FOR INCREASING PHYSICAL SECURITY.

a. By means of an AG letter, procedure was established for the investigation and clearance of telephone company employees for duties in connection with automatic enciphering equipment.

b. A policy was instituted whereby rules governing physical security of certain cryptographic machines are to be incorporated in classified instruction documents.

3. PROCEDURES FOR INCREASING TRANSMISSION SECURITY.

a. Monitoring activity was increased to include Pacific Ocean Areas, European Theater of Operations, United States Army Forces in the Middle East, and certain areas in and around the Mediterranean Theater. In October 1944 direction communication channels were established with monitoring stations 1 (Vint Hill Farms, Warrenton, Va.), 3 (Miami Beach, Fla.), 9 (Bellmore, L.I.), and 10 (Reseda, C.l.).

b. A standardized monthly report form (covering violations of transmission security, remedial action taken, monitoring missions assigned, etc.) was adopted.

c. Charts showing specific violations of radio transmission security, as found by analysis of monitoring logs, were distributed to violating units.

d. Scripts dramatizing actual violations of transmission security were prepared for reproduction as training recordings.

4. NEW DEVICES AND MACHINES PLACED IN SERVICE.

a. The speech equipment, AN/GSQ-1( ), was received from the manufacturers and distributed to several theaters. The equipment utilizes code cards, each of which provides security for 15 minutes.

COPY

b. The Converter M-325 was received from the manufacturer and distributed for trial use in certain areas. It is a hand-operated electromechanical device using a reversing rotor and three stepping rotors from a set of nine rotors (a set consists of one reversing rotor and eight stepping rotors). The rotors are so designed that their wiring may be changed at will.

c. The Converter M-218( )/U was placed in service at the State Department. It utilizes a special rotor basket and plugboard rotor, and provides semiautomatic operation cryptographically equal to Converter M-325.

5. NEW OR IMPROVED MACHINES IN DEVELOPMENT.

a. Converter M-294, which uses a new type of rotor and rotor basket, was received from the manufacturers.

b. Converter M-409 was developed, and will probably be available for service tests sometime in 1945. It is an electromechanical machine utilizing the same cryptographic principles as the Converter M-325, but is keyboard operated and tape printing.

c. Most of the development of speech equipment AN/GSQ-2 was accomplished; the equipment will be service tested in 1945.

d. Facsimile equipment AN/GXQ-2( ) was developed, and will be ready for use in trial installations in 1945.

e. Converter attachment AN/GSA-2 (Auto Converter M-134-C) was tested, and additional units will probably be procured in 1945.

f. The RADCO device, an improved version of SLIDEX, was issued for limited field tests.

6. MODIFICATIONS OR IMPROVEMENTS IN EXISTING MACHINES.

a. Modified Converter M-228 was developed; it is provided with a rotor stepping arrangement different from that of the standard converter. When used according to a special procedure, the Modified Converter afford non-repeating key operation, and is secure enough for radio transmission of TOP SECRET messages.

b. The new one-time tape system involves an improvement over the old system which used the 131-B-2 subset, a receiving transmitter distributor, and one form or another of teletype equipment. By modifying a receiving transmitter distributor (14AB) instead of the 131-B-2 subset, the same results were accomplished, thus leaving the subset standard. Closely connected to this improvement is the Universal Connection Block, by means of which it is possible to install both a Converter M-228 and one receiving transmitter distributor for one-time tape operation on a 131-B-2 subset.

7. ESTABLISHMENT OF NEW CRYPTONETS.

a. Cryptonets incorporating Converter M-228 systems were established as, for example, Cryptonet 38, which is for use in the transmission of weather, flight operational, and administrative traffic.

b. Cryptonet 41 was the first to include Converter M-325.

c. Three training cryptonets were made up for communication between Fort Monmouth and Camp Crowder.

8. IMPROVEMENTS IN CRYPTONETS.

a. The scope of existing and newly created cryptonets was enlarged to include all necessary types of cryptographic systems. For example, Cryptonet 21 was revised to include one-time tape, Converter M-134-C, strip, and Converter M-209 systems; and plans were made for a new cryptonet for Military Attaches and Military Intelligence Liaison Officers to include one-time pad, onet-time tape, strip, Converter M-325, and double transposition systems.

b. The over-all picture of cryptographic systems used in cryptonets has been clarified by the trend toward elimination of systems which were unnecessary, were little used, or could be combined with other existing systems; for example, the emergency double transposition systems which had been provided for the world-wide high command cryptonets were eliminated.

9. IMPROVEMENTS IN LIAISON.

a. In order to give greater assistance to the theaters, the production of AFCODE, a radiotelephone code developed in AFHQ, and the increased production of Converter M-209 were undertaken.

b. Because of the nature of certain CCB publications, the burden of publication is thrown on the individual services; in this there has been complete cooperation among the services concerned.

c. Permission was granted the British to use Converter M-228 in combined operations, provided that all maintenance is performed by U. S. Army personnel.

10. IMPROVEMENTS IN OPERATIONAL PROCEDURES.

a. Stencils are now cut by Electromatic typewriters in "G" Branch.

b. New "checking boxes" for use in checking stencils were instituted; use of these boxes has resulted in greater accuracy.

c. The electromechanical counterpart of Converter M-325 was used to a limited extent instead of Converter M-325 itself for making 26-30 and circuit checks.

11. SECURITY STUDIES.

a. A method was developed by which the rotors of Converter M-134-C may be reconstructed and traffic read on the basis of sufficient depth (approximately 10 messages). Several methods of solution of the Combined Communication Machine were discovered, resulting in a recommendation for a change in construction of rotors and in the adoption of a new indicator system. The wiring and stepping principles of Converter M-294 were based on specific machine studies.

b. A study of actual traffic cryptographed in various systems resulted in recommendations to improve authorized systems and in a drive to replace locally devised insecure authentication systems, Slidex, aircraft movement codes, etc., with secure systems.

c. Tactical monitoring logs were studied to determine violations of transmission security, quality of analysis made by the initial examining agency, quality of monitoring logs, call sign schedules and variations from prescribed radio procedure.

d. The results of a study of procedure for reporting compromise and cryptographic violations will be incorporated in a registered document.

e. A preliminary study (with recommendations) was made to determine what intelligence can be gleaned from call signs, system indicators, and internal message references.

12. NEW OR REVISED PUBLICATIONS.

a. Systems instructions were published as registered documents, as technical manuals, technical bulletins, and training circulars.

b. Effective date lists and current cryptographic information were published in the Monthly Informational Document.