

University of Nebraska - Lincoln
DigitalCommons@University of Nebraska - Lincoln

DOD Military Intelligence

U.S. Department of Defense


10-11-1942

FM 11-35, Signal Corps Intelligence, 1942

Robert Bolin

University of Nebraska-Lincoln, rbolin2@unl.edu

Follow this and additional works at: <https://digitalcommons.unl.edu/dodmilintel>

 Part of the [Defense and Security Studies Commons](#), [Military and Veterans Studies Commons](#), [Other Engineering Commons](#), [Peace and Conflict Studies Commons](#), and the [Soviet and Post-Soviet Studies Commons](#)

Bolin, Robert, "FM 11-35, Signal Corps Intelligence, 1942" (1942). *DOD Military Intelligence*. 113.
<https://digitalcommons.unl.edu/dodmilintel/113>

This Article is brought to you for free and open access by the U.S. Department of Defense at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in DOD Military Intelligence by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.

~~CONFIDENTIAL~~

FM
11-35
2 Sep 42

FM 11-35

WAR DEPARTMENT

SIGNAL CORPS
FIELD MANUAL

SIGNAL CORPS INTELLIGENCE

September 2, 1942

Handwritten:
Date 12/20/42
G-7A

~~CONFIDENTIAL~~

Handwritten:
DR. C. H. ... 38
1954

Property of
Office of the Chief
Military History
General Reference Branch

Property of U. S. Army

WAR DEPARTMENT,
WASHINGTON, September 2, 1942.

FM 11-35, Signal Corps Intelligence, is published for the information and guidance of all concerned.

[A.G. 062.11 (2-24-42).]

BY ORDER OF THE SECRETARY OF WAR:

G. C. MARSHALL,
Chief of Staff.

OFFICIAL:

J. A. ULIO,
Major General,
The Adjutant General.

DISTRIBUTION:

D (5) ; R and H (2) ; Bn and H 11 (5) ; C 11 (2) .
(For explanation of symbols see FM 21-6.)

TABLE OF CONTENTS

	Paragraphs	Page
CHAPTER 1. General.....	1-5	1
CHAPTER 2. Signal Intelligence Service.		
Section I. General.....	6-14	4
II. War Department.....	15-23	6
III. Army.....	24-30	11
CHAPTER 3. Signal Intelligence Service Procedure.		
Section I. Radio intelligence.....	31-35	14
II. Signal security.....	36-39	16
III. Secret ink laboratory.....	40-42	20
IV. Code and cipher compilation.....	43-46	21
V. Cryptanalysis.....	47-49	23
CHAPTER 4. Enemy Equipment Identification Service.		
Section I. General.....	50-52	26
II. Captured signal equipment.....	53-62	26
CHAPTER 5. Other Intelligence Duties Performed by Signal Corps.		
Section I. Censorship.....	63-68	30
II. Intelligence section.....	69	33
III. Operation in various theaters.....	70-72	33
APPENDIX I. Form of directive to radio intelligence company.....		35
II. Report forms.....		36
INDEX.....		39

RESTRICTED

SIGNAL CORPS FIELD MANUAL

SIGNAL CORPS INTELLIGENCE

CHAPTER 1

GENERAL

■ **1. PURPOSE.**—The purpose of this manual is twofold: to serve as a guide for Signal Corps personnel charged with the performance of signal intelligence duties, and to furnish information to commanders and their staffs as to the functions, responsibilities, capabilities, and limitations of signal intelligence.

■ **2. ORGANIZATIONS.**—Organizations for the specific performance of signal intelligence activities are available to the military commander of the field forces and to army and other subordinate commanders. Such organizations may be assigned to theaters of operations, defense commands, or task forces, as circumstances warrant.

■ **3. SIGNAL CORPS REPRESENTATIVE IN G-2.**—A Signal Corps representative should be assigned to the G-2 section of the general staff of armies and higher commands. It will be the responsibility of this officer to obtain, through G-2 channels, all available intelligence of hostile signal communication systems, including commercial wire and radio facilities.

■ **4. DEFINITIONS.**—To assure a thorough understanding of the terms used in this manual the following definitions are given:

a. Signal intelligence includes all information of the enemy obtained by radio or other electrical means, by the detection of secret inks and other disguised writings, by the solution of codes, ciphers, and other secret means of communication, and by the interception of visual communication. It does not include information obtained by sound, flash, or subaqueous ranging.

b. Signal security is the safeguarding of friendly communications against the availability and intelligibility of those communications to hostile or neutral intelligence agencies. It includes also the restricting of communications as far as possible to addressees or agencies directly concerned.

c. Signal Intelligence Service is a component of the signal service of higher commands which is specifically charged with the performance of certain signal intelligence activities. It is responsible for the supervision of signal security, and for the preparation and issue of certain cryptographic and other equipment used by the command.

d. Enemy equipment identification service is a component of the signal service of higher commands which is specifically charged with the recovery and evacuation of captured signal equipment and literature.

e. Radio intelligence is that part of signal intelligence which is obtained by means of radio equipment. It includes both position finding and intercept activities and is an exclusive duty of the signal radio intelligence company (Table of Organization 11-77).

f. Radio position finding is the procedure of locating on a map or aerial photograph the probable position of a radio transmitter through the intersection of plotted azimuths sensed by two or more specially designed radio receivers.

g. Radio intercept is a method of obtaining radio intelligence through the copying of hostile or neutral radio transmission and, when ordered, becomes a partial or secondary mission of all communication units. It does not include the intercepting of friendly transmissions.

■ 5. REFERENCES.—The publications and training films listed below contain general or specific references to the subject of signal intelligence:

FM 11-5, Mission, Functions, and Signal Communication in General.

FM 11-10, Organization and Operations in the Infantry Division.

FM 11-20, Organizations and Operations in the Corps, Army, Theater of Operations, and GHQ.

FM 11-25, Aircraft Warning Service.

SIGNAL CORPS INTELLIGENCE

FM 24-5, Signal Communication.

FM 30-5, Combat Intelligence.

FM 30-25, Counterintelligence.

FM 100-5, Operations.

FM 100-15, Larger Units.

Joint Action of the Army and the Navy.

AR 380-5, Safeguarding Military Information.

TF 11-205, Safeguarding Military Information -- Cryptographic Security.

TF 11-324, Safeguarding Military Information.

CHAPTER 2
SIGNAL INTELLIGENCE SERVICE

	Paragraphs
SECTION I. General-----	6-14
II. War Department-----	15-23
III. Army-----	24-30

SECTION I

GENERAL

■ 6. DUTIES.—The specific functions and duties of the Signal Intelligence Service may include any or all of the following:

a. Preparation, publication, storage, and distribution of codes and ciphers employed by our armed forces, and the repair and maintenance of cipher machines.

b. Interception of enemy radio and wire traffic by electrical means.

c. Location of enemy radio transmitting stations by radio position finding methods.

d. Solution of enemy codes and ciphers.

e. Development and preparation of secret inks to be employed by our own authorized agents and the detection of the presence of secret ink and other disguised writings in enemy documents.

f. Monitoring of friendly radio traffic in order to detect violations of signal security and the initiation of corrective measures.

■ 7. WAR DEPARTMENT.—The Signal Intelligence Service of the War Department is operated by the Chief Signal Officer to serve the military commander of the field force and his staff. The officer in charge of the Signal Intelligence Service is responsible for all of the duties outlined in paragraph 6. In addition to the personnel of the Signal Intelligence Service he has under his control such radio intelligence companies or detachments as may be required properly to perform his mission. (See FM 100-15.)

■ 8. THEATER OF OPERATIONS.—Organizations for the specific performances of signal intelligence activities may be allotted to expeditionary forces, defense commands, or task forces when the size of the force and the distances involved indicate the desirability of decentralizing signal intelligence activities. A portion of such organizations may be retained in a general reserve by the military commander of the field forces, for assignment as the situation dictates.

■ 9. ARMY.—A signal intelligence section is an integral part of the headquarters, signal service, army. The officer in charge of this section is responsible for the duties outlined in paragraph 4 which are within the capabilities and facilities of the section to perform. He has under his control the radio intelligence company assigned to the army.

■ 10. LOWER UNITS.—Signal Corps personnel within corps and divisions may be directed to assist in signal intelligence activities in addition to their signal communication duties. While signal intelligence is not a normal mission for signal communication personnel, all such personnel should be trained to recognize and immediately report any information of value to the signal intelligence effort. Examples of this type of information are violations of cryptographic security, heavy increases or silences in enemy radio transmission, description of captured or abandoned enemy signal communication or cryptographic equipment, intercepted enemy messages.

■ 11. RADIO INTELLIGENCE COMPANY.—The signal radio intelligence company is the basic information-gathering agency for signal intelligence. Through this unit the Signal Intelligence Service obtains the material for its study and evaluation.

■ 12. SPECIAL AGENCIES.—*a. Aircraft warning service.*—A highly specialized type of signal intelligence is furnished by the aircraft warning service. It is not a part of the Signal Intelligence Service of ground forces but a function under the direction of air force commanders. A detailed description of the aircraft warning service will be found in FM 11-25.

Censorship.—The Signal Corps is responsible for making the technical arrangements for the censorship of all electrical means of signal communication in the combat zone and in the communications zone if it is under martial law and to cover particular areas wherein censorship is established.

■ 13. ORGANIZATIONAL.—Table of Basic Allowances for Signal Corps prescribes certain equipment for issue to signal intelligence personnel and organizations. Radio intercept and direction-finding equipment is included therein. Secret and confidential cryptographic equipment issued by signal intelligence agencies to tactical organizations is not listed in Tables of Basic Allowances.

■ 14. SPECIAL EQUIPMENT.—Much of the equipment used by signal intelligence agencies is highly technical and secret. No authorized allowances of such equipment are prescribed. It is provided as needed and may include the following:

a. Tabulating machines for use in code compilation and in cryptanalysis.

b. Laboratory equipment and supplies for secret ink preparation and detection.

c. Equipment and supplies for cryptanalytic research and the development of new cipher devices.

d. Reproducing equipment and supplies necessary for the packing and shipping of codes, cipher machines, and cipher keys.

e. A library consisting of various technical books, dictionaries, periodicals, and other sources of general information.

f. Tools and supplies for the repair and maintenance of cipher machines.

SECTION II

WAR DEPARTMENT

■ 15. GENERAL.—The Signal Intelligence Service, War Department, operates under the direction of the Chief Signal Officer. It has under its control a varying number of radio intelligence companies (T/O 11-77) and fixed station radio intercept

detachments. The signal radio intelligence companies and fixed station detachments constitute a field force which gathers information over wide areas and places it at the disposal of the Signal Intelligence Service. The latter can be considered as a centralized laboratory which analyzes the material received and as rapidly as possible furnishes to the chief of staff, field forces, the concrete information obtained.

■ 16. DETAILED ORGANIZATION.—*a.* The Signal Intelligence Service is, in general, organized into sections as follows:

- Administrative section.
- Radio intelligence section.
- Security section.
- Laboratory section.
- Code and cipher compilation section.
- Code and cipher solution section.

b. A description of the organization of a signal radio intelligence company will be found in FM 11-20.

c. Certain additional organizations may be assigned to the Signal Intelligence Service for such purposes as interruption of wire lines, wire tapping, and photographic missions. The composition, size, and equipment of these detachments will depend upon the particular circumstances of their employment.

■ 17. OFFICER IN CHARGE.—The officer in charge of the War Department Signal Intelligence Service is an assistant to the Chief Signal Officer. He is responsible to the Chief Signal Officer for the operation of the Signal Intelligence Service including assigned and attached radio intelligence companies. In the name of the Chief Signal Officer he issues such orders and directives as may be necessary to the radio intelligence companies and other organizations which may be assigned for signal intelligence duties. He has direct supervision over all activities of the Signal Intelligence Service. He maintains liaison with such members of the G-2 section of the War Department General Staff as are concerned with the functions of signal intelligence, and with the approval of the Chief Signal Officer, is the technical adviser to G-2 on such matters.

■ 18. ADMINISTRATIVE SECTION.—The Administrative section is responsible for the administration and supply of the Signal Intelligence Service. The officer in charge of this section assists the officer in charge of the Signal Intelligence Service in the supervision of all activities and in securing prompt and effective operation. The section is responsible for all correspondence between the Signal Intelligence Service and other offices or organizations. The securing of special technical equipment not provided through normal supply channels is a responsibility of this section.

■ 19. RADIO INTELLIGENCE SECTION.—This section is responsible for the technical supervision of the War Department radio intelligence companies. It carries out this responsibility by performing the following duties:

a. Preparation of plans for the interception of radio traffic and location of enemy transmitters to include directives to be given the radio intelligence companies. See appendix I for a suggested form for such directives.

b. By agreement with the security section, the preparation of plans and directives to the radio intelligence companies for the monitoring of friendly traffic.

c. Submission to the code and cipher solution section of intercepted enemy traffic and cooperation with that section to insure that cryptographed messages in the quantity and type needed to facilitate solution are made available.

d. Evaluation of information received from the position-finding activities of the radio intelligence companies to include probable location of stations, call signs, frequencies, net coupling, and any peculiar operating characteristics.

e. Submission of daily reports to G-2 on volume of traffic, movement of stations, and radio silences, to assist him in evaluating all information and in determining the enemy's capabilities.

f. Submission to the security section of reports on violations of signal security obtained by monitors.

g. Preparation of plans for the coordination of the activities of radio intelligence companies assigned to armies and subordinate commands in order that duplication may be

avoided and that the position-finding and intercept units of all the field forces may function as a team.

■ 20. SECURITY SECTION.—The security section has the primary mission of detecting and preventing violations of signal security. It has a secondary mission of planning for wire interruption and wire tapping. It carries out its missions by performing the following duties:

a. Preparation of plans in collaboration with the radio intelligence section for the monitoring of friendly radio traffic.

b. Study of reports furnished by the radio intelligence section on instances of signal security violation including violations of cryptographic security to determine the extent of damage done.

c. Preparation of corrective orders and disciplinary measures aimed at preventing violations of security.

d. Advising the code compilation section when cryptographic systems have been compromised in order that replacements may be issued and the compromised systems rescinded.

e. Preparation of plans and directives for the employment of dummy radio stations, sending of false messages, and other methods of radio deception.

f. Preparation of plans and directives for the use of wire tapping and wire interrupting detachments.

g. Provision of proper safeguards to prevent the enemy from tapping or interrupting friendly wire lines.

■ 21. LABORATORY SECTION.—The laboratory section operates a secret ink laboratory. It is charged with both the development and detection of secret inks and cryptic methods other than code or cipher. It performs as required the following duties for G-2:

a. Preparation and issue of secret inks for use by intelligence agents.

b. Examination of documents suspected of containing secret ink, microphotography, or other espionage methods of writing.

c. Examination of mail of suspected enemy agents where the fact of such examination is desired to be kept unknown.

d. Preparation of photostatic or photographic copies of evidence against espionage agents which have been obtained by the secret inks laboratory.

■ 22. CODE AND CIPHER COMPILATION SECTION.—The responsibilities of this section include the following:

a. Compilation, production, and distribution of codes and ciphers in use by the field forces.

b. Issue and maintenance of cipher machines.

c. Preparation and issue of instructions covering the employment of cryptographic systems.

d. Periodic issue of cipher keys for systems used in signal communication.

e. Provision of secure storage for reserve cryptographic equipment.

f. Notification to all agencies concerned of the effective date of changes in cryptographic systems.

g. Destruction of superseded cryptographic equipment.

■ 23. CODE AND CIPHER SOLUTION SECTION.—The code and cipher solution section will be organized into a number of subsections depending upon the number and type of enemy cryptographic systems under study. In general its duties are—

a. Analysis of intercepted enemy messages in code and cipher for the purpose of solving enemy systems.

b. Translation of messages in systems which can be solved.

c. Indexing and filing of all intercepted enemy traffic.

d. Preparation in cooperation with the radio intelligence section of plans for the interception of the particular type of enemy traffic desired.

e. Submission to G-2 of the translations of solved messages.

f. Furnishing to the signal intelligence services of armies and any other subordinate commands all available material to permit local translation of intercepted messages.

g. Preparation of technical reports on new cryptanalytic methods for instructional and historical purposes.

h. Technical coordination of the solution activities in all subordinate signal intelligence companies.

i. Design and development of equipment for cryptanalytic employment.

SECTION III

ARMY

■ 24. GENERAL.—The Signal Intelligence Service assigned to an army consists of the signal intelligence section of the headquarters, signal service, army (T/O 11-200-1) plus one or more radio intelligence companies (T/O 11-77). Special wire detachments for tapping or interrupting wire lines may be provided from time to time. The signal intelligence section is strictly an operating agency. It is not organized to perform any of the research or production duties of the Signal Intelligence Service of the War Department.

■ 25. DETAILED ORGANIZATION.—The signal intelligence section being much smaller and having more limited duties than the corresponding service of the War Department, no definite suborganization is prescribed. Subsections will be set up corresponding to the duties performed and the following four subsections would normally be found:

- Administrative.
- Radio intelligence.
- Security.
- Solution.

■ 26. OFFICER IN CHARGE.—The officer in charge of the army signal intelligence section is an assistant to the army signal officer. He is responsible to the army signal officer for the supervision and conduct of signal intelligence activities within the army. In the name of the army signal officer he issues orders and directives to the one or more radio intelligence companies assigned to the army. With the approval of the army signal officer he maintains close contact with the G-2 section of the Army general staff and acts as technical adviser to G-2 on signal intelligence matters. He exercises direct control over the signal intelligence section. He cooperates with the Signal Intelligence Service of the War Department under whose technical supervision he functions to attain the necessary coordination of all signal intelligence agencies of the field forces.

27. ADMINISTRATIVE SUBSECTION.—The administrative subsection is responsible for the supply and administration of the signal intelligence section. The officer in charge of this subsection assists in the general supervision of all army signal intelligence duties. The handling of all correspondence between the signal intelligence section and other offices or organizations is a responsibility of this subsection.

■ 28. RADIO INTELLIGENCE SUBSECTION.—The radio intelligence subsection exercises technical supervision over the one or more radio intelligence companies assigned to the army. It is responsible for the following duties:

a. Preparation of plans for the interception of enemy radio traffic and location of enemy transmitters, to include directives to be given the radio intelligence companies. See appendix I for a suggested form for such directives.

b. By agreement with the security subsection, the preparation of plans and directives to the radio intelligence companies for the monitoring of friendly traffic.

c. Submission to the solution subsection of intercepted enemy traffic which can be translated without lengthy cryptanalytic study.

d. Submission to the administrative subsection of intercepted enemy traffic which cannot be translated for forwarding to the Signal Intelligence Service of the War Department.

e. Evaluation of information received from the position-finding activities of the radio intelligence companies to include probable location of stations, call signs, frequencies, net grouping, and any peculiar operating characteristics.

f. Submission of daily reports to G-2 based on volume of affic, movement of stations, and radio silences, to assist him in evaluating all information, and in determining the enemy's capabilities.

g. Submission to the security subsection of reports on violations of signal security obtained by monitors.

■ 29. SECURITY SUBSECTION.—The security subsection is responsible for the following duties:

a. Study of reports furnished by the radio intelligence subsection on instances of signal security violations, including

violations of cryptographic security, to determine the extent of damage.

b. Preparation of corrective orders and disciplinary measures aimed at preventing violations of signal security.

c. Informing the Signal Intelligence Service, War Department, of compromised cryptographic systems.

d. Preparation of plans and directives for the employment of dummy radio stations, the sending of false messages, and methods of radio deception as directed by G-2.

e. Preparation of plans and directives for the use of wire tapping and wire interrupting detachments and the initiation of action to obtain such detachments.

f. Provision of proper safeguards to prevent the enemy from tapping or interrupting friendly wire lines.

g. Receipt from the Chief Signal Officer and distribution within the Army of such cryptographic equipment and replacements as may be issued from time to time.

■ 30. SOLUTION SUBSECTION.—This subsection, unlike the code and cipher solution section, Signal Intelligence Service, War Department, does not perform original cryptanalysis. It is dependent upon the latter for material enabling the decryptographing of enemy traffic. Its primary duties are—

a. Decryptographing and translating of enemy messages in systems for which the solution has been furnished by the War Department.

b. Arranging with the radio intelligence subsection for the maximum interception of traffic in known systems.

c. Submission to G-2 of the translations of messages.

d. Maintenance of close contact with the Signal Intelligence Service of the War Department on all matters affecting solution activities.

CHAPTER 3

SIGNAL INTELLIGENCE SERVICE PROCEDURE

	Paragraphs
SECTION I. Radio intelligence.....	31-35
II. Signal security.....	36-39
III. Secret ink laboratory.....	40-42
IV. Code and cipher compilation.....	43-46
V. Cryptanalysis.....	47-49

SECTION I

RADIO INTELLIGENCE

■ 31. GENERAL.—Radio intelligence is the most prolific source of signal intelligence information. It is of two forms: radio intercept and radio position finding. The radio intelligence companies have been organized for the sole purpose of securing this type of information. Radio intelligence companies are assigned as an organic part of each army. They may also be assigned to defense commands, task forces, or other special missions. They are sometimes employed independently for frontier or coast defense or for counterintelligence in the zone of the interior. It should be noted that their disposition is based on technical and not tactical decisions. The primary consideration governing all radio intelligence operations is that information be placed at the disposal of commanders in sufficient time for effective countermeasures.

■ 32. COMPANY.—The organization, duties, and operating methods of the radio intelligence company are discussed in detail in FM 11-20.

■ 33. RADIO INTERCEPT.—Radio intercept is made of messages in the clear and messages in code or cipher. Clear text messages are normally only of immediate action value and individually of minor importance; taken in volume they frequently give an indication of enemy dispositions and probable

lines of action. The decision as to value, however, should not be made by the intercepting operator but by the officer responsible for the intercept directive. If the directive calls for guarding a certain frequency or channel, all traffic heard should be copied and submitted. If the directive asks for specific types of traffic, only those types need be copied, although any traffic heard which is of known value should be copied whether covered by directive or not. When speed of transmission, volume of traffic, or weak signals render direct copying difficult, transmissions are recorded on equipment provided for the purpose and transcribed by the intercepting agency at the earliest opportunity. All intercept is of value only if it is handled speedily. Intercepted traffic normally is sent by messenger from the intercepting agency to the Signal Intelligence Service under which it operates. Frequent scheduled messenger service must be established. Telephone or telegraph should be used to supplement the messenger service, particularly in cases requiring urgent action. The use of radio to forward intercepted traffic is inadvisable.

■ 34. RADIO POSITION FINDING.—Radio position finding is dependent upon close cooperation between radio intercept stations and radio direction-finding stations. The radio intelligence company functions as a team composed of direction-finding stations and intercept stations. The intercept stations locate enemy signals by searching a limited portion of the radio spectrum or by guarding certain channels. A located signal is reported by telephone to the direction-finding stations and simultaneous bearings are taken. The determination of probable position is accomplished by plotters assigned to the control section. Radio direction finding is based on the two facts that radio waves travel in great circular paths, and that a properly constructed rotatable receiving antenna will give minimum response when its plane is at right angles to the direction of the radio wave. In taking bearings two sources of error are present: first, the inability of the operator to locate the exact point of minimum response; second, the fact that radio waves are affected by the presence of electrical conductors, terrestrial irregularities,

called "magnetic storms," and other factors which cause refractions in the great circle paths. Careful analysis based on locally obtained data will assist in reducing this second type of error, but it must always be assumed to be present and to increase with the radio frequency of the signal. Consequently, highly accurate results in position finding cannot be expected. It is generally safe to assume that each bearing is accurate to within 10°. The probable location is determined from the plotting of three or more azimuths.

■ 35. **SIGNAL SECURITY MISSIONS.**—Signal security missions are frequently assigned to the intercept sections of the radio intelligence company. These missions consist of the monitoring of friendly radio stations in accordance with directives furnished by the Signal Intelligence Service. In monitoring a friendly station or net all transmissions are copied but normally only those about which there is a question as to signal security violation are forwarded to the Signal Intelligence Service. The usual violations of signal security are—

- a. Unauthorized or unwarranted transmission of radio messages in the clear.
- b. Improper use of cryptographic systems.
- c. Violation of radio silence.

SECTION II

SIGNAL SECURITY

■ 36. **CRYPTOGRAPHIC.**—Codes and ciphers, unless properly used, cannot be expected to provide security against enemy intelligence. AR 380-5 sets forth the basic rules governing use of cryptographic systems. In addition, each code or cipher system is generally accompanied by instructions which apply specifically to that system. No person should attempt the use of any cryptographic system unless and until he is thoroughly familiar with both the general and specific instructions. The life of any code must be considered fairly short, since there are many opportunities for physical compromise. Cipher systems are designed so that their cryptographic security lies in a changeable key and the system may remain in effect, after compromise, by simply changing the

key. Cipher systems, while offering greater flexibility, are generally more vulnerable to hostile cryptanalysis. Enciphered code will provide the greatest security, but it is usually too slow for field use. It is the duty of the Signal Intelligence Service to provide suitable cryptographic systems, to insure their proper use by instruction and by monitoring, and to effect immediately the replacement of systems which have been compromised.

■ 37. RADIO.—The radio transmitter is the most prolific source of intelligence in field operations. Radio transmission in the clear is justified only in situations when the time available to the enemy is insufficient for exploitation of the information contained in the message. (See FM 24-5 and 100-5.) Under no circumstances should personal convenience affect the decision to send in clear. Time is the only consideration. Radio should be considered as an auxiliary means of communication supplementing wire and messenger service. Under many conditions radio is the only possible means but if choice exists wire or messenger is to be preferred. Radio security consists not only of guarding what is transmitted, but of limiting the use of radio to actual necessity. Enemy intelligence may be served by every transmission from a friendly station. Even though the message may be unintelligible, every transmission must be assumed to disclose the identity of both transmitting and receiving stations, and the location of the transmitting station (and of the receiving station also if the message is acknowledged). It is for this reason that radio silence is frequently ordered prior to the actual commencement of offensive operations. To enforce radio security the Signal Intelligence Service is responsible for the monitoring of friendly radio transmissions and the initiation of corrective or disciplinary measures where necessary.

■ 38. WIRE.—While immeasurably safer than radio, wire communication is not completely reliable from the security viewpoint. It is not secure against enemy espionage agents. With some types of wire lines physical tapping may not be necessary, for interception can be accomplished by electric induction. This is particularly true of ground return cir-

cuts. Interception by induction, however, requires the presence in the vicinity of the wire line of detecting and amplifying equipment. By the enforcement of proper measures, wire communication can be accorded a fairly high degree of security. These measures consist of—

a. Policing wire lines by electric means.—By the use of test sets the attempt at wire tapping on any line frequently can be detected. When an unauthorized telephone is cut in on a line the electric characteristics of the line are slightly changed. This change may be detected on the meter of a test set.

b. Surveillance on the part of operators.—All operators should be trained to challenge any suspicious voice or sound indicating the presence on the line of unauthorized listeners. The circumstances should be immediately reported to the wire chief for investigation.

c. Use of armed guards.—Armed guards should be detailed to police the length of any wire lines believed to be in danger of interception. It is the only defense against interception by induction, which cannot be detected by electric means.

d. Training of using personnel.—Regardless of the safeguards employed, no wire line of normal length can be considered as perfectly secure. All personnel must be cautioned against discussing on the telephone any information of vital importance. All secret messages should be cryptographed before transmitting by telegraph.

9. AUTHENTICATION.—One of the most important and effective of all security measures is the use of authentication, which has a twofold purpose. It assures the recipient of a message that the transmitting agent is *bona fide*; conversely, it assures the transmitting agent that the recipient is *bona fide*, which is equally important. To be effective, authentication should be applied to each message rather than periodically between transmitting and receiving agencies. Too much dependence should not be placed on recognizing voices. The fidelity of radio voice transmission is frequently poor and the sound of a familiar voice can be imitated by enemy agents. Few personal characteristics are inherent in telegraphic transmissions either by radio or wire, and without

some means of authentication the recognition of transmissions as bona fide is impossible. It is a responsibility of the Signal Intelligence Service to provide suitable authentication systems when required. The authenticator group is transmitted in the heading of the message or, in the case of voice transmission, immediately after contact has been established. An insecure authentication system which the enemy may solve and use is worse than none at all, for it causes reliance to be placed on a false message which might otherwise have been questioned. Authentication systems possessing the desired degree of security fall generally in one of the following two classes:

a. Prearranged lists.—A list of words, letters, or numerals is prepared and furnished all correspondents. The words, letters, or numerals are then used in regular order, one at a time, to authenticate each message. When once used, the authenticator is crossed off the list and not used again. This method is particularly effective between two correspondents. As the number of correspondents increases it becomes more difficult for any one correspondent to select the next authenticator on the common list. In such cases the correspondent attempting to establish his identity can be given the last used authenticator and told to supply the following one.

b. Additive method.—A more flexible method applicable to a large number of correspondents is that involving the principle of addition. According to a key furnished all correspondents, a numerical cipher is substituted for the letters of the alphabet and is employed as indicated below. Assume the following numerical cipher to be in effect:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4	8	5	6	2	0	1	3	7	9	0	5	2	4	3	8	1	0	7	2	6	3	9	4	9	2

The receiving operator challenges the transmitting operator by asking him to authenticate any three letters at random, for example, **KRP**. The transmitting operator adds the numerical equivalents of these letters and replies "8." He may then challenge the receiving operator to ascertain that the person or station answering is the intended receiver of the message, for example, asking him to authenticate **BXS**. When the reply "19" is given, authentication has been established between both parties.

SECTION III

SECRET INK LABORATORY

■ 40. PREPARATION OF SECRET INKS.—A secret ink laboratory operates under the signal intelligence division, War Department, and theater of operations. The officer in charge of the laboratory section directs the activities of the secret ink laboratory. One of the duties with which the laboratory is charged is the preparation of secret inks for the use of such intelligence agents as may be authorized by the Assistant Chief of Staff, G-2. The laboratory instructs these agents in the use of the ink, furnishes them with a supply for their mission, develops communications received from such agents, and prepares communications addressed to them. The composition of secret inks and the manner of their use and development is secret information and cannot be covered in this manual.

■ 41. DETECTION OF SECRET INKS.—A more continuous activity of the laboratory is the examination of suspected documents for the presence of secret ink. In some cases the fact of such examination is purposely concealed from the addressee of the document. In others the secret writing must be photographed to provide permanent evidence of its existence. This is frequently a difficult operation, due to the dimness or very short period of legibility of the writing. The secret ink laboratory assists in censorship work in the theater of operations by examining suspected documents. It assists in setting up facilities for secret ink detection in such locations as may be directed by the officer in charge of censorship and provides technical supervision over such examining stations. The methods used in secret ink detection are covered in secret documents prepared by the Chief Signal Officer.

■ 42. OTHER ACTIVITIES.—In addition to secret inks there are many other methods of transmitting information, the detection of which requires laboratory analysis. Among the more common of such methods are—

a. *Microscopic writing.*—This can be performed only by a highly skilled person. By using a pen or some other instrument, minute writing is inscribed on a hair, a grain of rice,

or other appropriate object. Engraving may be applied to glass or similar hard polished substance. Such methods, while frequently undetectable to the naked eye, may be discovered by microscopic examination.

b. Microphotography.—A highly successful method requiring no artistic skill employs microphotography. By this method a letter-size piece of paper is photographed on specially prepared film and reduced to small dimensions.

c. Invisible photographs.—A photographic print can be rendered invisible by applying a certain chemical solution. In transit the print appears as a blank piece of paper or may contain visible writing to avoid suspicion. The recipient is able to restore the original print by applying to it the proper chemical solution.

d. Writing under stamps.—A common method is that of writing in small script and pasting a postage stamp over the writing. This method may be detected in a number of ways.

SECTION IV

CODE AND CIPHER COMPILATION

■ 43. CODE COMPILATION.—Codes are of two kinds. A *one-part* code is a list of code groups and corresponding meanings both arranged in alphabetical order. A *two-part* code consists of two lists; in the first or *encoding section* the meanings are arranged alphabetically and the corresponding code groups are assigned in random order; in the *decoding section* the code groups are arranged alphabetically and opposite each appears its meaning. The compilation of a two-part code is more of a task but such a code possesses far greater cryptographic security. Code groups are selected from a permutation table which is prepared for each code and shows the possible combinations of letters. It provides for sufficient dissimilarity between groups to avoid erroneous meanings resulting from telegraphic errors. A revision of a one-part code cannot be made without changing the permutation table. Successive editions of a two-part code may be compiled with the same permutation table by simply shuffling the groups. The use of tabulating machinery is indispensable in code

compilation. The Signal Intelligence Service has full technical responsibility for code compilation; it shares a joint responsibility with the using arms and services for the selection of adequate and concise plain text meanings. The using arms and services should make recommendations whenever necessary for the addition or deletion of meanings.

■ 44. CIPHER SYSTEMS AND KEYS.—Cipher systems fall into two general classes. In a *substitution cipher* the letters of the plain text are replaced by cipher equivalents as determined by a key. In a *transposition cipher* the letters of the plain text are retained but their relative position is changed in accordance with a *key*. The key is an element of variable nature which controls or directs encipherment and decipherment. It frequently consists of an easily remembered word, phrase, or group of numbers. A combination of the two methods is sometimes employed. The preparation of a cipher consists therefore of two elements: a description of the method to be employed and a list of keys. When a code becomes compromised the issue of a new code book becomes necessary, whereas the compromise of a cipher in general compromises only a particular key. Because of their simplicity in handling, cipher keys are changed frequently. No cipher system should be issued without at least one emergency key which can be put into effect upon notification. Cipher systems may be applied to encoded messages to increase security. This practice is normally followed when compromise of the code book is suspected and immediate replacement of the code is not possible.

■ USE OF TABULATING EQUIPMENT.—The preparation of codes and certain types of cipher keys is greatly facilitated and much time is saved by the use of tabulating machines. The operation of these machines requires the services of officer and enlisted personnel who have had experience with tabulating equipment. The method of using the tabulating machines is beyond the scope of this manual.

■ 46. CIPHER MACHINES.—In addition to the manually employed cipher methods mentioned in paragraph 44, cipher devices or machines are used for the purpose of increasing

both security and speed. Some of these devices are of rather complicated construction and present the same problem of maintenance as radio apparatus. Since these devices are secret or confidential, they are not handled through normal supply channels. The Signal Intelligence Service is responsible for the issue and replacement of this equipment. Trained personnel to make repairs, a shop with necessary tools and equipment, and a supply of spare parts for replacement are included in the Signal Intelligence Service, War Department, and theater of operations.

SECTION V

CRYPTANALYSIS

■ 47. GENERAL.—The principles of cryptanalysis are covered in a series of War Department text books entitled "Military Cryptanalysis," parts I to IV. Cryptanalysis is an analytical science. A successful code and cipher solution section requires personnel trained in this science. Much of the work is clerical in nature, however, and a successful solution section may be built around a few expert cryptanalysts assisted by an adequate force of competent clerks. The translation of messages in systems which have been solved is expedited by the use of labor-saving devices and other special equipment. The use of equipment as well as many of the cryptanalytic procedures is secret information and is contained in secret technical manuals.

■ 48. BASIC OPERATIONS.—Four basic operations govern all cryptanalytic procedure. They are—

a. Determination of language.—Normally this presents no great problem in field operations as it may be assumed to be the mother tongue of the enemy. In the case of messages intercepted from espionage agents the determination may not be so simple. Indications of a particular language may be found in the heading or signature and in the absence of certain letters or the addition of accented letters. If the language cannot be determined, cryptanalysis proceeds and the language is determined later.

b. Determination of general system.—This is by far the most difficult phase of cryptanalysis and success cannot be

attained without a determination of the general system employed. It requires an exhaustive study of available text with the elimination, one by one, of cryptographic methods of known characteristics which do not apply. Errors on the part of enemy code clerks are most helpful in this determination. Information gathered from other intelligence agencies may also be of great value. Once the system has been determined, a definite plan of attack can be made and cryptanalysis may then proceed along intelligent lines with a definite objective in view.

c. Reconstruction of specific key.—Cryptographic systems other than straight code depend for their security upon a specific and changeable key which will still afford protection when the basic system has been discovered. The reconstruction of the key or keys used in messages under study must therefore precede or advance concurrently with the reconstruction of plain text. Generally the reconstruction of one key will assist in the reconstruction of others, and a cryptographic system cannot be considered as solved unless messages can be read in at least a majority of the keys used.

d. Reconstruction of plain text.—In this step the assistance of a qualified linguist in the language used is essential, for frequently assumptions of words must be made. Correct assumptions can be proved when tested against the general system and the proved or assumed specific key. When completely reconstructed and proved, the plain text is translated into English if the original message was in a foreign language.

■ 49. RESULTS.—*a. Time.*—It must be remembered that successful cryptanalysis cannot be given a time limit. Solution depends to a large extent on intelligent recognition and application of information supplied through the errors of enemy code clerks. Ultimate solution of cryptographic systems cannot be expected in all cases. Success is normally attainable only as a result of long and patient study aided by such "breaks" as the enemy may afford through misuse of his cryptographic systems.

b. Accuracy.—The accuracy of results attained by the solution of enemy messages should be emphasized. Successful application of cryptanalytic principles in effecting solution

provides results whose accuracy cannot be doubted. In other words, cryptanalysis produces results which are entirely correct or it produces no result at all. The procedure is based upon the absolute check of each assumption made and consequently the final result is a product of cross-checked elements. The highest reliability can be placed on information obtained through the solution of cryptographed enemy messages.

CHAPTER 4

ENEMY EQUIPMENT IDENTIFICATION SERVICE

	Paragraphs
SECTION I. General.....	50 62
II. Captured signal equipment.....	53 62

SECTION I

GENERAL

■ 50. PURPOSE.—A unit known as the Enemy Equipment Identification Service (EEIS) operates under the direction of the Chief Signal Officer. A section of the EEIS is attached to the headquarters signal service of higher commands for the purpose of effecting recovery of and evacuating captured signal equipment and literature.

■ 51. ORGANIZATION.—The EEIS is organized so as to be capable of providing each field army or separate task force with a headquarters of not less than four officers, at least one of whom shall be of field grade, and the necessary complement of enlisted men; and of providing each separate division and corps with a detachment of not less than one specially trained officer and the necessary specially trained enlisted personnel.

■ 52. DUTIES OF UNIT.—The duties of this unit are described in section II. Additional duties may be assigned from time to time by the Chief Signal Officer.

SECTION II

CAPTURED SIGNAL EQUIPMENT

■ 53. ACTION BY CAPTURING ECHELON.—*a.* The handling of captured cryptographic equipment is of special importance. The capturing echelon will transmit codes, ciphers, and cipher devices to the enemy equipment identification officer without delay and report as provided in *c* below. Keying

mechanisms or other essential elements should remain undisturbed.

b. Captured signal communication instruction books on all other captured signal equipment will be reported immediately by capturing echelon to the enemy equipment identification officer.

c. The report by capturing echelon will include (see Appendix II for preliminary report guide) :

- (1) Type and/or description of equipment.
- (2) When captured.
- (3) Where captured.
- (4) Present location.

■ 54. ASSIGNMENT OF OFFICER TO STUDY AND REPORT.—The army or task force signal officer to whom captured instruction books or other signal communication equipment are reported will assign an officer from the EEIS to make a study of the captured matériel and to prepare a detailed report with sufficient copies for distribution as required. The report on captured matériel will conform to the form prescribed by the Chief Signal Officer (see appendix II for detailed report guide) and will be accompanied by photographs, drawings, etc. Rubbings, tracings, or copies of the name plate and part or component marks will be made whenever these are in a foreign language.

■ 55. CLASSIFICATION.—The enemy equipment identification officer upon completion of his report on captured matériel will classify the captured equipment as "for study," "utilization," "salvage," or "destruction."

■ 56. CAPTURED ENEMY EQUIPMENT CLASSIFIED FOR STUDY.—
a. Equipment so classified will include prototypes of new equipment and equipment utilizing new or different materials or improvements in the arrangement of component parts. At least two sets in good working condition will be classified for study although prototypes have been so classified previously.

b. The enemy equipment identification officer will report through the army or task force signal officer direct to the Chief Signal Officer by wire, radio, or cable a brief description of any new equipment and also advise the means of

transportation by which set or sets are being sent. (See par. 61.)

■ 57. CAPTURED ENEMY EQUIPMENT CLASSIFIED FOR UTILIZATION.—Equipment so classified will be placed in working condition and used for—

- a. Interception.
- b. Counterintelligence.
- c. Deception of the enemy.
- d. Supplementing our own communication system in local theaters.
- e. Such other use as may be directed.

■ 58. CAPTURED ENEMY EQUIPMENT CLASSIFIED FOR SALVAGE.—Equipment so classified will be dismantled and usable components and materials will be listed as spare parts for equipment marked "utilization" or will be used to augment our own supply of spare parts when such parts are interchangeable.

■ 59. CAPTURED ENEMY EQUIPMENT CLASSIFIED FOR DESTRUCTION.—Equipment so classified will be utterly destroyed so that repair, salvage of parts, or identification is impossible. Destruction will be accomplished by mechanical, electrical, pyrotechnical, or other suitable means as directed by the enemy equipment identification officer.

■ 60. PRISONERS OF WAR.—Prisoners of war may be—

- a. Interrogated by both the enemy equipment identification officer to augment his report and by the army or task force signal officer to devise for better operation and utilization of the captured equipment.
- b. Sent to designated points in the communications zone or zone of the interior where enemy equipment and technical matters are being tested or studied in order that our own technicians may benefit by their special knowledge.

■ 61. PROTOTYPES TO OFFICE OF THE CHIEF SIGNAL OFFICER.—The army or task force signal officer of the operating tactical unit in a theater of war or the senior signal officer of an area will, upon receipt of the enemy equipment identification officer's report, send two prototype sets of captured communication equipment (see par. 56) to the Chief Signal Officer by the quickest means of available transportation. The equip-

ment should be sent as two shipments rather than as a single shipment. If only one item of a type is captured, it should be sent immediately to the Chief Signal Officer, not waiting for a second prototype. As soon as another one is captured, the second item should be sent.

■ 62. INFORMATION REQUIRED BY OFFICE OF CHIEF SIGNAL OFFICER.—The following factors will be included in the report forwarded to the Chief Signal Officer. Sufficient copies of the report will be prepared for distribution, as required.

- a.* Methods and procedure used by the enemy.
- b.* Equipment materially different from ours.
- c.* Degree of standardization and simplification.
- d.* Type of personnel using the equipment.
- e.* Materials used in the equipment.
- f.* Methods of issuing equipment and technical data.
- g.* Methods of handling spare parts.
- h.* Unit to which the equipment was assigned.
- i.* Methods enemy uses to destroy equipment.
- j.* In what quantities enemy uses equipment.
- k.* Samples of captured manuals, maps, charts, other paraphernalia.

CHAPTER 5

OTHER INTELLIGENCE DUTIES
PERFORMED BY SIGNAL CORPS

	Paragraphs
SECTION I. Censorship.....	63-68
II. Intelligence section.....	69
III. Operation in various theaters.....	70-72

SECTION 1

CENSORSHIP

■ 63. **GENERAL.**—The Signal Corps is responsible for making technical arrangements for the censorship of all electric means of signal communication in the combat zone, and in the communications zone if it is under martial law. Necessary censorship is exercised over the personal communications of military personnel and in some cases over commercial telephone, telegraph, and radio communications, including broadcasting. The Signal Corps assists in censorship by developing and printing all news and other photographs leaving the

combat zone (see FM 30-25). The secret ink laboratory may be called upon to render assistance to the G-2 representative in the examination of documents.

■ 64. **WRITTEN MESSAGES.**—The censorship of written messages (cablegrams, radiograms, telegrams) may be handled generally as follows:

a. All channels leading out of the theater of operations will be closely supervised. Wire lines which cannot be properly censored will be interrupted. Radio channels which cannot be censored will be discontinued. In effect censorship should make a completely isolated locality of the theater of operations.

b. Censorship stations should be located at the centers of radio and wire communication.

c. All persons desiring to send messages out of the theater of operations will be required to submit the message to the censor for check. The censor should require complete identification of the individual and make an evaluation of his trustworthiness, since an apparently innocent message may contain military information through the medium of a pre-arranged code.

d. It is a responsibility of the Signal Corps to insure that only properly authorized messages are transmitted via communication facilities under Signal Corps control.

■ 65. RADIO BROADCASTS.—The censorship of radio broadcasting will require—

a. Submission by the radio station of complete script for approval prior to transmission.

b. Monitors at each transmitting station. The monitors will be given complete copies of approved scripts and will be able immediately to interrupt the transmission if there is any departure from the approved script.

c. Preparation of transcriptions prior to broadcast of any program which cannot easily be reduced to script. Only approved transcriptions are broadcast.

■ 66. TELEPHONE COMMUNICATION.—a. *Calls out of theater of operations.*—Any civilian desiring to make a call out of the theater of operations must obtain authority from the censor by personal appearance at the toll office. The censor should require adequate identification, evaluate the applicant's trustworthiness, and instruct him as to what may and what may not be said over the telephone. The call should then be monitored by a censor who is able to break the connection at will.

b. *Local calls within the theater.*—Whether there is to be censorship, surveillance, or interruption of local telephone service in friendly or occupied enemy territory is a command decision.

c. *Toll calls within the theater.*—The censorship of all toll calls is advisable, since information may be relayed by this means for later passage to enemy hands.

d. Military telephone calls.—Instructions relative to security measures in telephonic communication should be issued to all military personnel. Surveillance of military calls must be exercised to insure that the instructions issued in the interests of security and counterintelligence are being observed. Military calls within the theater should be checked by a sampling method and all personnel should be cautioned that their conversations will be subject to censorship. Recording apparatus should be made available for this purpose. Military calls are not subject to interruption by censors but disciplinary action should be taken against personnel who have been found to violate security regulations without adequate reason.

■ 67. DETECTION OF UNAUTHORIZED RADIO STATIONS.—In continental United States and certain oversea territories or possessions the Federal Communications Commission assumes the responsibility for the detection and location of unauthorized radio transmitters. In a theater of operations the Signal Corps is responsible for this action. Should territory of the United States become a theater of operations any and all civilian monitoring or intercept agencies may be placed under the control of the Signal Corps. In friendly territory such civilian agencies may be continued in operation augmented by radio intelligence units furnished by friendly sources. In hostile territory the entire task falls to Signal Corps radio intelligence units. Unless some special need exists, all radio transmitting stations in the theater of operations except legitimate broadcasting stations should be closed and sealed. If needed, they should be operated only by Army or Navy personnel.

■ 68. PHOTOGRAPHS.—All photographic negatives taken by official or accredited civilian photographers in the theater of operations will be sent to a Signal Corps photographic laboratory for development. The photographs will then be censored by a representative of G-2. No photographs, negatives, or prints will be released except by the authority of the theater commander after they have been examined. A Signal Corps photographic laboratory is set up under

the direction of the chief of staff, field forces. When the theater of operations includes a wide area, such small auxiliary laboratories as may be needed to provide prompt and efficient photographic censorship will be provided. The secret ink laboratory (see pars. 40 to 42, incl.) is also equipped to develop and print photographs but its duties in this respect are limited to counterespionage and do not normally include routine censorship.

SECTION II

INTELLIGENCE SECTION

■ 69. COMMUNICATION INFORMATION.—*a.* The gathering of information concerning the signal communication facilities of hostile as well as friendly or neutral countries is of high importance. Among the items of particular interest are—

(1) Lay-out of telephone systems to include location of centrals, capacity, and routing of open wire lines and cable, and the type of central office and substation equipment used.

(2) Location, power, frequency, and call letters of radio transmitting stations.

(3) Availability and kind of electric power.

(4) Organization and equipment of signal or communication troops of other armies, friendly as well as hostile.

b. In addition to the above items which are concerned only with signal communication, other widely varied items are of interest to the Signal Intelligence Service and are frequently of utmost importance to the success of the code and cipher solution section.

SECTION III

OPERATION IN VARIOUS THEATERS

■ 70. UNITED STATES TERRITORY.—When the theater of operations is confined to territory of the United States it may be assumed that civilian governmental agencies will continue to function as far as practicable. If necessary they may be placed under military control. Such agencies as

the Weather Bureau, the Treasury Department, the Federal Communications Commission, and the Department of Justice are able to perform many of the security and intelligence functions which would otherwise be a responsibility of the Signal Corps. Signal intelligence plans should contemplate the use of the widespread and highly organized intelligence and counterintelligence nets of such agencies to the fullest extent. Signal intelligence agencies should be devoted more or less exclusively to the service of the armed forces in the field. Special radio intelligence missions for border or seacoast defense may require the services of a large number of radio intelligence companies. The cooperation between military and civilian agencies should be of the highest degree in order that duplication of effort be avoided and military personnel released to provide a mobile force ready to serve the commander of the field forces.

■ 71. ALLIED COUNTRIES.—As far as practicable, use should be made of security and intelligence agencies provided by the allied country. The close cooperation to be expected from our own governmental agencies will rarely if ever be found in allied countries and the responsibilities of the Signal Corps for providing adequate security and intelligence measures become greater. In such matters as code book solution, secret ink detection, and radio position finding, close cooperation between our signal intelligence service and that of the allied government is desirable. Cryptographic means for the exchange of messages between our own and allied forces must be provided. Duplication of many of the signal intelligence activities between our own and allied agencies is to be expected and in many respects cannot be avoided unless unity of command over all forces is established.

■ 72. ENEMY TERRITORY.—The Signal Corps is responsible for all phases of signal intelligence and security in enemy territory. Cooperation with existing civilian facilities is not possible and consequently a large force of radio intelligence personnel will be required. Security measures assume

INDEX

	Paragraph	Page
Agencies of signal intelligence:		
Army	9	5
General	2	1
Lower units	10	5
Radio intelligence company	11	5
Signal intelligence service	7	4
Special agencies	12	5
Theater of operations	8	5
Censorship:		
Detection of unauthorized radio stations	67	32
General	63	30
Photographs	68	32
Radio broadcasts	65	31
Telephone communication	66	31
Written messages	64	30
Code and cipher compilation:		
Cipher machines	46	22
Cipher systems and keys	44	22
Code compilation	43	21
Use of tabulating equipment	45	22
Cryptanalysis:		
Basic operations	48	23
General	47	23
Results	49	24
Definitions	4	1
Duties:		
Signal Intelligence Service, Army:		
Administrative subsection	27	12
Officer in charge	26	11
Radio intelligence subsection	28	12
Security subsection	29	12
Solution subsection	30	13
Signal Intelligence Service, General	6	4
Signal Intelligence Service, War Department:		
Administrative section	18	8
Code and cipher compilation section	22	10
Code and cipher solution section	23	10
Laboratory section	21	9
Officer in charge	17	17
Radio intelligence section	19	8
Security section	20	9
Enemy equipment identification service:		
Captured signal equipment:		
Action by capturing echelon	53	26
Assignment of officer to study and report	54	27
Captured enemy equipment, classified for—		
Destruction	59	28
Salvage	58	28
Study	56	27
Utilization	57	28

INDEX

Enemy equipment identification service—Con.		
	Paragraph	Page
Captured signal equipment—Continued.		
Classification	55	27
Information required by the Office of the Chief Signal Officer.....	62	29
Prisoners of war.....	60	28
Prototype to Office of the Chief Signal Officer.....	61	28
Duties of unit.....	52	26
Organization	51	26
Purpose	50	26
Equipment:		
Organizational.....	13	6
Special	14	6
Intelligence section:		
Signal communication information.....	69	33
Organization:		
Signal intelligence service, Army:		
Detailed.....	25	11
General.....	24	11
Signal intelligence service, War Department:		
Detailed.....	16	7
General.....	15	6
Purpose of manual.....	1	1
Radio intelligence:		
Company.....	32	14
General.....	31	14
Radio intercept.....	33	14
Radio position finding.....	34	15
Signal security missions.....	35	16
References.....	5	2
Secret ink laboratory:		
Detection of secret inks.....	41	20
Other activities.....	42	20
Preparation of secret inks.....	40	20
Signal security:		
Authentication.....	39	18
Cryptographic security.....	36	18
Radio security.....	37	17
Wire security.....	38	17
Signal intelligence in various theaters:		
Allied countries.....	71	34
Enemy territory.....	72	34
United States territory.....	70	33