RESTRICTED

AS-14
AS-23 AS-22 Aug 3 1949 FM 32-( ) "Communication Intelligence and
AS-80 Communication Security"

Capt. Campbell Ext 317

1. Inclosed herewith in first draft of Chapter I of the proposed FM 32-( ), Communication Intelligence and Communication Security," currently being prepared by Lt. F. A. Geb, Jr., at Fort Monroe, Virginia.

2. It has not been indicated to AS-22 whether paragraph 2 has been omitted purpose, will be inserted later, or whether this is an error in numbering.

3. It is requested that this chapter be reviewed and that limited comments on the writer's approach to the subject be forwarded to AS-22 by 10 August 1949.

4. It is to be pointed out that when completed, the entire manual will be coordinated thoroughly within the Agency.

1 Incl (in trip)
Draft, subj as above

CHARLES H. HISER
Lt. Colonel, Signal Corps
Acting Deputy Chief
Army Security Agency

---

2 AS-22 AS-14 11 Aug 49 Mr. Rhoads/Ext 215

Lt. Geb's approach as indicated in this draft is excellent. Some minor changes are indicated in the text.

1 Incl
Draft, subj
as above

WILLIAM F. FRIEDMAN
Special Assistant to the Chief,
Army Security Agency

SIS DATE 11 Aug 49 SIG

RESTRICTED

TOP SECRET SECRET CONFIDENTIAL RESTRICTED

OFFICE OF THE SPECIAL ASSISTANT
TO THE
CHIEF, ARMY SECURITY AGENCY

DATE 4 May

TO		FROM
✓	Mr. Friedman	
	Mr. Rhoads	✓
	Capt. Lane	
	Dr. Pettengill	
	Dr. Conder	
	ASA Review	

( ) As discussed
( ) As requested
( ) Concurrence or comments
( ) Information & forwarding
( ) Information & return
( ) Information & file
( ) Info upon which to base reply
( ) Recommendation
( ) Signature if approved
( ) Your action by

I think Gebs approach here
10 May 49 is very good. Have
indicated a few changes
Yes, I agree OK. WFF
will do a good job, I think. F

This should be a very useful Field Manual when finished. I think the approach and treatment of the material is excellent.

I noticed paragraph 2 is missing. Perhaps there is a mistake in numbering?

There are two places in the text I believe needs reworking. The first is paragraph 5a on page 6. Here he has used the word artfulness where I believe another word would be better. To me the word usually means cunning, crafty, wily, or tricky. He undoubtedly means skill in design, or skill in use.

The second place is at the top of page 10. Lt. Geb is apparently confused concerning the relationship between degree of security and ease of operation. As you know well, degree of security depends upon the cryptographic principle employed and the operation of the system may or may not be simple. For example, compare the M-209 and SIGTOT.

TOP SECRET SECRET CONFIDENTIAL ~~RESTRICTED~~

OFFICE OF THE SPECIAL ASSISTANT
TO THE
CHIEF, ARMY SECURITY AGENCY

DATE 4 Aug

TO		FROM
__	Mr. Friedman	___
__	Mr. Rhoads	✓
__	Capt. Lane	___
__	Dr. Pettengill	___
✓	Dr. Conder	___
__	ASA Review	___
__	_____	___
__	_____	___
__	_____	___

( ) As discussed
( ) As requested
( ) Concurrence or comments
( ) Information & forwarding
( ) Information & return
( ) Information & file
( ) Info upon which to base reply
( ) Recommendation
( ) Signature if approved
( ) Your action by

This is a draft of 1st section of manual being written by [illegible]
10 May 49
[illegible]. Would like your comments, regarding our approach. [illegible]

~~RESTRICTED~~

DRAFT

FM 32-( )

COMMUNICATION INTELLIGENCE

AND

COMMUNICATION SECURITY

DRAFT

~~RESTRICTED~~

FOREWORD

Modern war is notable principally for the range, speed and flexibility of its operations which have been made possible by great technological advancements. The complexity of today's warfare has compounded the need of commanders at all echelons for effective intelligence services.

Experience has demonstrated that enemy signal communications constitute the most prolific single source of intelligence which has been available to the Army. By the same token, it must be recognized that our own communications are potential sources of intelligence to others. Consequently, the closely interrelated fields of communication intelligence and communication security, the former concerned with producing intelligence from the communication of the enemy, and the latter dealing with our measures to forestall unauthorized access to information in our own communications, have assumed great importance in the scheme of National Defense.

Today, as warfare approaches a completely scientific stage of development, a general understanding of the capabilities and limitation of both of these fields must be possessed by all personnel whose assignments involve the establishment, operation, or use of military communication systems in order that the very substantial contributions which the Army's communication intelligence and security efforts are capable of making to the success of military operations may be fully realized.

~~RESTRICTED~~

This manual supersedes chapters and , FM 11-35, 2 September 1942

SECTION I

GENERAL

1. PURPOSE AND SCOPE. The purpose of this manual is twofold: first, to assist commanders and their staffs in the prosecution of their missions by furnishing information which will enable them to use communication intelligence and communication security services to maximum effect, and second, to serve as an operating guide to communication intelligence and security personnel and units in the execution of their missions in support of military operations. This manual covers the fundamentals of communication intelligence and security, and the divisions of responsibility which have been established for the production and utilization of communication intelligence and the maintenance of communication security. The various communication intelligence and security services available to the commander are described, as well as the methods which are employed to control their operations. The capabilities and limitations of specific communication intelligence and security techniques and type units are discussed to assist in the preparation of intelligence and counterintelligence plans and directives. Throughout this manual, statements of doctrine are accompanied by discussions of the facts and circumstances which underlie the doctrine. This practice has been followed to emphasize the need for the strict observance of principles or established practices when the consequences of non-observance are not self-evident.

~~RESTRICTED~~

SECTION II

INTRODUCTION

3. GENERAL.

a. The bona fide communications of a military force are the most accurate, timely sources of information which exist concerning its plans and capabilities. They contain virtually all the information which must be exchanged to insure the successful execution of operations.

b. Important information is usually reduced to written or graphic form and transmitted by an appropriate means. The means of communication which are employed vary from simple visual or sound systems to complex electrical transmission systems. When more than one means of communication is available, the specific means to be employed is determined principally by the distance which separates the correspondents and the speed of communication which may be necessary or desirable.

c. Modern military operations are characterized by great mass and flexibility which have been made possible, in large measure, by the development of electrical means of signal communication. The rapidity of transmission, traffic handling capacity, and ease of installation of certain electrical means have contributed directly to the development of tactics which are capable of sweeping entire continents, in continuous coordinated actions involving forces deployed over extended fronts, often with no physical links between them.

d. The dependence of command upon signal communication is in direct proportion to the scale and mobility of operations. The means of signal communication which are employed to exercise control are dictated by and adapted to the nature and size of the operation undertaken. Intelligence is gathered, plans are formulated and coordinated, men and materiel are massed and moved, battles are launched, controlled and won through the web of signal communication which enables the commander to be completely informed of the tactical situation as it develops, and to remain in control of his forces although physically separated from them.

e. But no means of transmission, however efficient or versatile, is inherently secure from interception. In guileless hands, the electrical means of signal communication, especially, are two-edged swords. In a figurative sense, they ordinarily afford no greater privacy from the eavesdropper than the human voice. Radio, on which modern tactical operations lean so heavily, is a booming voice which addresses friend and foe, alike. Unprotected and indiscriminate electrical communication transmissions tell the interceptor with matchless accuracy of the organization, plans, and capabilities of his adversary.

f. Foreknowledge of the enemy's intentions and capabilities is the principal objective of all military intelligence operations, and often the key to success. Insofar as the friendly military effort is concerned, the usefulness of the most efficient communication systems is seriously impaired if they are permitted to become free sources of intelligence to the enemy. Therefore, the employment of communications as instruments of unmixed advantage is a military objective of paramount importance.

g. The communication security effort of the Army is directed to the end that its communications shall give undivided service to the friendly cause. The purpose of the Army's communication intelligence activities is to employ the communications of the enemy as instruments to his speedy and decisive defeat.

4. RELATIONSHIP BETWEEN COMMUNICATION INTELLIGENCE AND SECURITY. Historically, the exploitation of communications for their intelligence value, and the invention and application of protective measures were almost wholly uncoordinated. From the viewpoint of the modern army, its communication intelligence and security activities are complementary and mutually dependent. Coordination of communication intelligence and security activities, at all echelons, is accomplished through technical channels which exist to facilitate complete and rapid exchanges of information. Weaknesses which enable the exploitation of enemy communications are called to the attention of communication security specialists who examine friendly communications for similar weaknesses and devise effective countermeasures. Conversely, communication intelligence specialists are appraised of newly discovered security principles and developments in equipment and procedures in order that these may be considered in the attack on current communication intelligence problems. Studies to determine the suitability for adoption of new security procedures oftentimes are joint communication intelligence and security enterprises. Thus the full power of each activity is exerted to effect improvements in the other.

5. COMMUNICATION INTELLIGENCE VERSUS COMMUNICATION SECURITY OF OPPOSING FORCES.

a. In any situation, the ascendency of communication intelligence over communication security, or vice versa, depends on the relative cryptologic development of the opposing forces. Ordinarily, attacks on the security of communications are successful in proprotion to the experience and resourcefulness of communication intelligence agencies and the scale on which their operations are conducted. Impregnability of security, on the other hand, is proportional to the artfulness of communication security procedures, the state of training of signal communication personnel, the discretion with which interceptable means of communication are employed, and the comparative technical immaturity of opposing communication intelligence forces. It follows, then, that the security of communications is always relative, and sometimes an unknown quantity.

b. The objective of communication intelligence services is to choose and to use at will those communications which are of the greatest assistance to the friendly military effort. The objective of communication security activities is to reduce the communication intelligence effort of opposing forces to impotence by providing military information, passed by the various means of communication, with immunity from access by unauthorized persons for the duration of its useful life.

c. Efforts to protect or exploit communications take their direction from the frequency with which given means of transmission must be used and the vulnerability of those means to interception.

Means which are employed to effect the physical transmission of communications provide the greatest protection from interception because the communications which they are employed to transmit usually remain in the custody of trusted personnel who, by their vigilance, effectively prevent their exposure to the enemy. Except in unusual circumstances, means for the physical transmission of communications do not lend themselves to systematic exploitation and therefore yield little intelligence. Transmissions by sound and visual means of signal communication offer greater opportunities for interception, but, although their security is a matter of continuing concern to the using force, the volume and value of the traffic which is passed by these means is usually insufficient to warrant the establishment of special, coordinated intercept programs. In contrast, electrical means of signal communication, especially radio, carry large volumes of immediately important and potentially useful information and, of all means, are the most vulnerable to interception. Their indispensability to the conduct of military operations causes the success or failure of the communication intelligence and security efforts of any army to be measured in terms of the assistance to its cause which is obtained from electrical signal communications, hostile and friendly.

d. The principal factors in signal communication which provide the occasions for contest between the communication intelligence and security activities of opposing forces are the:

(1) Need for speed in communication.

(2) Widespread use of electrical communication and the opportunities which they offer for interception.

(3) Vulnerability of radio communications to position finding techniques.

(4) Tendency of signal communication networks to parallel command channels and to reveal functional relationships.

(5) Need for standard communication procedures.

(6) Incidence of human error.

6. SPEED VERSUS SECURITY.

a. The requirement for speed in military communication is as fundamental as the need for communication, itself. The invention and perfection of electrical means of communication has satisfied the requirement for speed. Their vulnerability to interception has been accepted as a risk which is justified by the rapidity of transmission which they offer.

b. The increased danger of interception which has accompanied the adoption of electrical means of communication has stimulated the development of procedures to guarantee the security of the information which they are employed to transmit. Communication security procedures are designed, insofar as possible, to preserve the efficiency of the signal communication system. At the present stage of development, the application of security measures is usually separate rather than simultaneous with transmission and, under normal operating conditions, acceptable standards of speed and security can be maintained by well trained communication personnel. In urgent tactical situations, speed may become of such overriding importance that security must be abandoned

as a secondary consideration, but in each such instance, the injury which is avoided by the relaxation of security must be greater than the immediate or long range consequences which may result from the exposure of classified information to interception by the enemy.

c. The need to preserve the efficiency of signal communications at the expense of their security is the bridge which enables the invasion of the security of every communication system.

7. SIGNAL COMMUNICATION TRANSMISSIONS.

a. Signal communication transmissions, as a whole, are composed of two basic elements:

(1) The texts of messages which military correspondents desire to exchange.

(2) The communication procedures which have been invented to facilitate the transmission and delivery of messages by the agencies of signal communication.

b. The texts of messages exchanged by military correspondents are the primary objects of the attentions of both communication intelligence and security specialists. Cryptosystems are applied to the texts of messages to render them unintelligible when they contain classified information and are to be transmitted by interceptable means. Cryptosystems are graded in accordance with their inherent ability, under proper usage, to withstand cryptanalytic attack. They are distributed throughout the military organization in accordance with predetermined requirements for security and intercommunication.

Low grade systems are used where short term security is adequate and simplicity of operation is a prerequisite. Stronger cryptosystems are reserved for use at higher levels where electro-mechanical simplicity is less important, long term security is mandatory, and important security principles can be preserved from serious risk of capture. Cryptanalytic techniques vary with the cryptosystems under attack. The rate at which solution proceeds usually conforms to the system's inherent level of security. General solutions for cryptosystems become increasingly complex and time consuming as the enemy matures cryptologically.

c. As sources of intelligence, communication procedural transmissions are second only to the texts of messages which are transmitted by electrical means of signal communication. The mutual incompatibility of speed and security in communication is nowhere more clearly emphasized than in the development of communication procedures. They must facilitate the establishment of communication, and enable the transmission and delivery of messages with speed and security. Yet, efficiency is achieved by complete standardization of procedures, and security is nurtured by change. The functions of procedural elements must remain constant, although their identities may be disguised by cryptographic methods. Severe limitations are imposed on attempts to improve the security of communication procedures because signal communication operators are incapable of memorizing or otherwise coping with frequent, complete changes in the identities of procedural elements. Consequently, only those elements which are the most immediate sources of intelligence are disguised. The result is a

mixture of plain and cipher elements which, in combination with data from radio position finding and special indentification operations, yields extensive order of battle information and contributes to intercept and cryptanalytic activities.

d. It is a fact that all emissions from electrical means of signal communication, whether they are intended to convey information or not, are sources of intelligence. All successful communication intelligence and security efforts are built on this foundation.

NOTE:

At this point a detailed treatment of the fundamentals of communication intelligence will be introduced. Communication security will be treated in the section immediately following. Then there will be a discussion of the organization and functions of the Army Security Agency. The manual will be closed with a discussion of the capabilities and limitations of communication intelligence and security field type units.