U. S. ARMY SIGNAL SCHOOL
FORT MONMOUTH N. J.

SSTS 56002A
INFORMATION SHEET
OFFICERS' DEPARTMENT

COMMUNICATIONS SECURITY (COMSEC)

Section I. GENERAL

1. OBJECTIVES

a. To discuss the principles of communications security (COMSEC) and their importance.

b. To discuss ways and means of achieving communications security.

c. To discuss areas of responsibility in COMSEC planning, COMSEC operations and enforcement of COMSEC regulations.

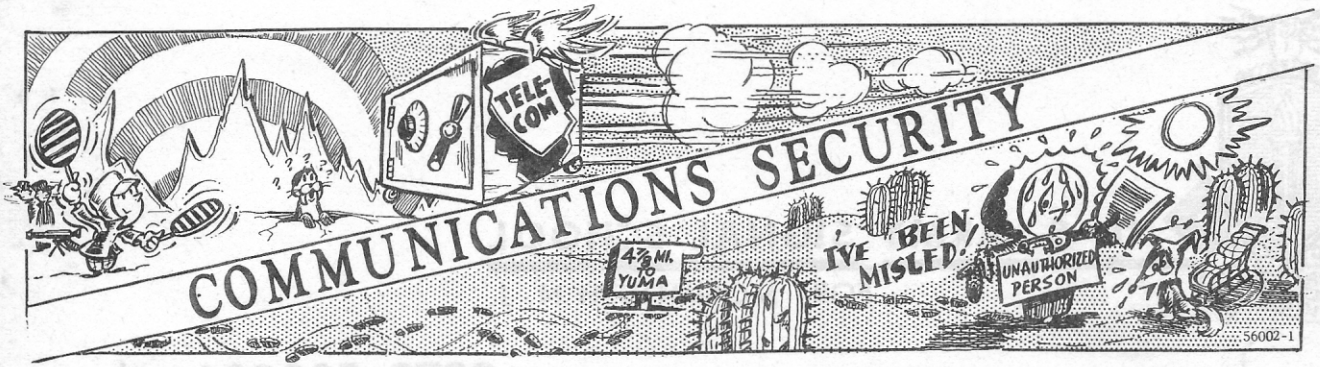
2. INTRODUCTORY INFORMATION

a. A primitive tribe raiding another tribe at the dawn of history had little need for communications in the modern sense. The chief gathered his warriors, told them where they were going, and controlled them by his voice during subsequent operations. He had little need to guard those communications from the enemy. The enemy were too busy guarding themselves to be able to make much use of intercepted intelligence.

b. Modern global warfare, with its new concept of dispersal, cannot be conducted by such a simple method. Today's communications -- and their protection from interception -- are vital to victory in battle. Strikes by many arms at many points require planning, and plans must be communicated. Unlike the sound of the chief's voice, such communications must precede action by considerable time. The enemy can usually intercept them in time to plan a counterattack or other defense, unless we take proper precautions.

c. Communication, then, is a reversible weapon. We cannot win battles unless we enable our forces to receive vital intelligence. And we cannot win battles if the enemy can receive this intelligence as readily as we. Communications security, therefore, is an integral part of communications, and we cannot discuss one without the other.

Supersedes SSTS 56002, Communications Security.



3. WHAT IS COMMUNICATIONS SECURITY?

a. Communications security is defined as the protection resulting from all measures designed to deny to unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such a study.

b. From the definition, it is clear that --

(1) Communications security is protection, which is the end result.

(2) COMSEC doesn't happen by chance; instead, it is the result of carefully designed measures.

(3) The purpose of COMSEC is to deny unauthorized persons valuable information that could be obtained from studying our communications. (The enemy constitutes only a part of the larger category termed unauthorized persons.)

(4) Full protection is not achieved as long as unauthorized persons are able to study our communications; it appears, therefore, that as long as we have electrical transmissions over radio and wire circuits we do not have ideal COMSEC.

4. PLAIN LANGUAGE PROBLEMS

a. The average person is under the false impression that information must be classified to be of significant intelligence value. The majority of our COMSEC problems stem from excessive and indiscriminate use of electrically transmitted unclassified messages. Such messages contain a vast amount of information which, item by item, is unclassified by all security standards. Yet through electrical transmission in plain language, particularly by radio, this information is readily available in sufficient volume to be of great value to unfriendly countries in times of peace, or to an enemy in time of war.

b. In this connection, we should explore the area of unclassified logistical and administrative messages transmitted by radio (and other electrical media). Because of operational requirements and lack of adequate cryptocapabilities to resolve conflicts between speed and security, vast quantities of information concerning friendly operations are susceptible to unfriendly interception. This problem has evolved from the U. S. Army's enormously complex system of procurement, processing, and movement of military supplies and personnel. Logistical and administrative traffic must frequently be transmitted over vulnerable radio channels. As a result, many items of significant intelligence value are exposed to interception and exploitation by unauthorized persons. After interception, this traffic can be compiled and analyzed in an easy, economical manner by linking project numbers with associated nicknames, names of personnel with associated units or organizations, and requisition numbers with shipping designators.

c. There is no doubt that unfriendly nations are collecting and studying U. S. Army plain language traffic, nor that the information so gained is being used in planning offensive or defensive action against the United States. In 1957, a Soviet major general stated in a Soviet publication that the USSR's defense against U. S. missiles would consist of preemptive blows on the launchers before the missiles could be fired. Another high-ranking officer stated that the USSR's most effective defense against U. S. long-range rockets would be by their destruction in the storage places, on the paths of their transports, and on the launching platforms. Unfortunately, much of the information that would enable the Russians to locate these storage places, transportation routes and launching platforms is being revealed in the tremendous volume of unclassified messages transmitted in the clear over U. S. Army circuits.

d. During World War II, a German prisoner of war said, "If U. S. troops win the war it will be in spite of their communications security and not because of it."

e. COMSEC becomes increasingly important each year, and it is an integral part of our communications. We must expend every effort in furthering COMSEC to reduce a serious threat to the security of the United States.

5. COMPONENTS OF COMMUNICATIONS SECURITY

Communications security has three essential components: transmission security, physical security and cryptographic (crypto) security. Each of these components will be defined and discussed in detail in succeeding portions of this text.

Section II. TRANSMISSION SECURITY

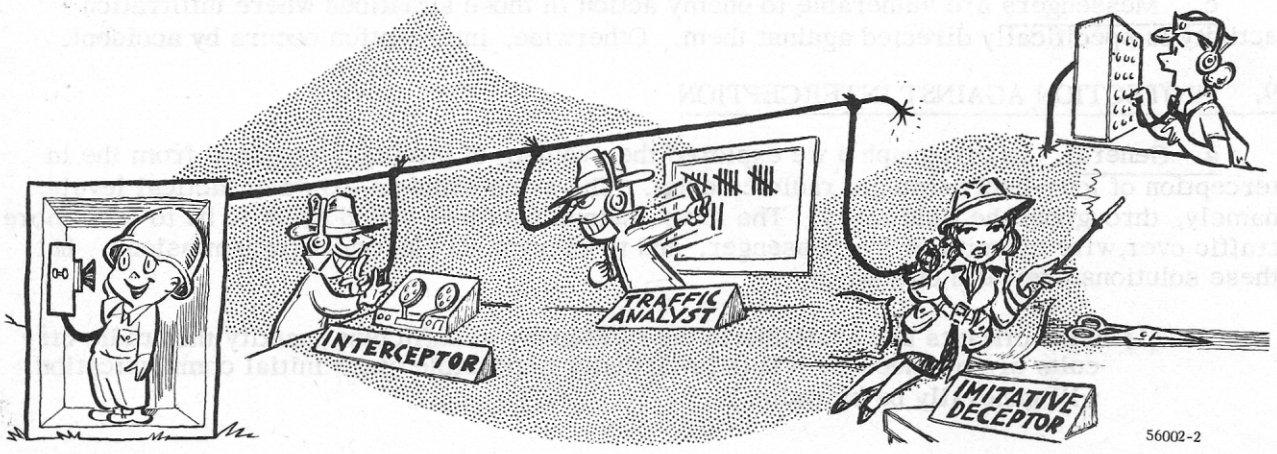
6. GENERAL

Transmission security results from all measures designed to protect transmissions from interception, traffic analysis, and imitative deception.

a. Interception is the act of listening in on and/or recording communications intended for another party for the purpose of obtaining intelligence.

b. Traffic analysis (T/A) is the technique of obtaining intelligence from the study of communications traffic without recourse to cryptanalysis.

c. Imitative deception is the introduction of fraudulent transmissions, which imitate authentic transmissions, into communications channels of an opposing force.



7. BACKGROUND

To understand clearly this component of COMSEC, we must think of our transmission media and the information being passed (transmitted) over these media. This means thinking in terms of --

a. Radio circuits (voice, radiotelegraph, teletypewriter, facsimile, and data).

b. Wire circuits (voice, teletypewriter, facsimile, and data).

c. Radio-wire integrated circuits (voice, teletypewriter, radiotelegraph, facsimile, and data).

d. Air messenger (fixed- and rotary-winged craft).

e. Motor messenger.

f. All others, such as semaphore, wig-wag, pyrotechnics, panels, pigeons, etc. (NOTE: These are not discussed in this text because of their rather limited application.)

8. VULNERABILITY TO INTERCEPTION

We have learned that interception is defined as the act of listening in on and/or recording communications intended for another party for the purpose of obtaining intelligence. One very important addition to this definition would be an act by the enemy physically incapacitating a messenger in order to obtain the material being transmitted. Every commander, communications officer and communications user must clearly understand the susceptibility of his transmissions to interception, whether they be sent by radio, wire, or messenger.

a. Radio is extremely vulnerable to interception; consequently all COMSEC plans and training directed toward radio users and operators must be accorded special emphasis. The extreme vulnerability of radio communications makes them a primary target of unfriendly intelligence agencies. Distance is usually no problem in the interception of radio communications. All that is required is a suitable place for the reception of emanated signals and sufficient trained personnel to intercept, analyze and compile resultant intelligence reports.

b. Wire communication is rightly considered to be more secure than radio, but only because interception of radio transmissions is so much easier, not because wire lines (circuits) are free from interception. To fully realize the vulnerability of a wire circuit, the user must know whether such a circuit is connected at some point to a radio circuit by patching or switching. This mode of operation is typical in some divisional communication systems. Such a circuit must be treated as a radio circuit insofar as transmission security is concerned.

c. Messengers are vulnerable to enemy action in those situations where infiltration activity is specifically directed against them. Otherwise, interception occurs by accident.

9. PROTECTION AGAINST INTERCEPTION

a. General. In paragraph 4 we explored the problem of intelligence gained from the interception of long-haul strategic radio circuits. The same problem exists at tactical levels; namely, throughout the field army. The most obvious solutions would seem to be to send more traffic over wire circuits or by messenger, and to encrypt all electrical transmissions. But these solutions are valid only when --

(1) Wire circuits are available to the field army in sufficient quantity that radio circuits are not needed. (This is virtually impossible since initial communication will generally be by radio.)

(2) The traffic is of such a precedence (ROUTINE or DEFERRED) as to permit transmission by messenger.

(3) The distances involved in transmission by messenger are not great enough to negate the precedence.

OR

(4) There exist sufficient cryptofacilities to encrypt all electrical transmissions.

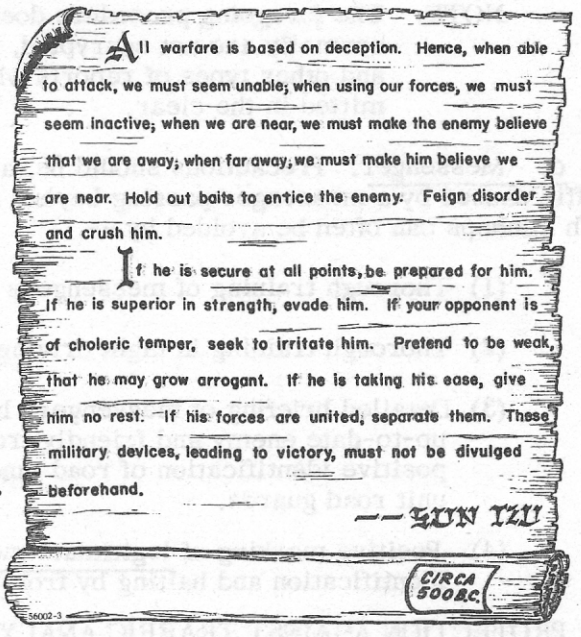
b. Radio. In tactical situations it must be assumed that interception of radio occurs every time a transmitter is operated; therefore, transmission security is a constant consideration when radios are used. The enemy obtains information merely by knowing that radios are operating. He obtains intelligence through traffic analysis (see paragraph 10). To achieve greater tactical surprise by denying such intelligence to the enemy, the commander may order radio silence or listening silence.

(1) In radio silence both radio transmitters and receivers are turned off. Generally, one of two methods is used to resume operations: by prearrangement (at a particular time, after a particular event, etc.) or through notification by some other means of communications.

(2) In listening silence radio transmitters are turned off, but receivers are operated for monitoring purposes.

(3) The commander must make the choice of radio silence or listening silence; the latter is generally used, since it allows radio nets to be made fully operative, without delay, upon receipt of a properly authenticated order or prearranged message from the commander.

(4) To be considered in COMSEC planning is the fact that very often either method of silence may produce an adverse effect -- the "silence" may provide the enemy with vital combat information. To counter this possibility, the wise commander and his signal/communications officer will prepare a well-coordinated deception plan. Such a plan might provide for control and manipulation of radio communications within the unit (or net) to conceal from the enemy the true time of attack or other planned action. Frequent periods of radio silence followed by controlled traffic may be used to deny the enemy the actual time of the planned action.



(5) Communications deception is a specialized field and is given full treatment in classified publications. It cannot be stressed too strongly that activity in this field is to be avoided by the novice.

c. Wire. Wire circuits are designated as either approved circuits or nonapproved circuits.

(1) An approved circuit is one designated by appropriate authority for the transmission "in the clear" of classified information of a specific security classification, except TOP SECRET. (In accordance with AR 380-5, under NO circumstances will TOP SECRET material be transmitted by electrical means unless encrypted.) Specific details concerning approved circuits, including procedures, approving authority(ies), safeguards and limitations are contained in ACP 122, Communications Security (U).

(2) A nonapproved circuit is any circuit not specifically designated for the transmission of classified information in the clear. Such a circuit may be used in simulated or actual combat operations to transmit any information except TOP SECRET when, in the judgment of the commander or his authorized representative, time cannot be spared for encryption and the enemy cannot exploit the information contained in the text. Specific handling procedures, as contained in AR 380-40, are as follows:

(a) Each such message or transmission will carry the words AUTHORIZED TO BE TRANSMITTED IN THE CLEAR over the signature of the commander or his authorized representative.

(b) The word CLEAR will be transmitted as the first word of the text.

(c) The received message will be marked with the phrase RECEIVED IN THE CLEAR prior to delivery. Such messages will be handled as at least CONFIDENTIAL material and will not be retransmitted. Should it be necessary to transmit the information to another addressee, a separate message will be originated and handled as the situation dictates.

NOTE: The foregoing procedure does not apply to messages which normally are not encrypted, such as enemy contact reports and other types of reports which are authorized to be transmitted in the clear.

d. Messenger. Precautions should be taken against accidental interception of messenger traffic caused by a messenger passing beyond friendly lines without knowledge or warning. Such mishaps can often be avoided by --

(1) Thorough training of messengers in map reading.

(2) Thorough training in night driving/flying.

(3) Detailed briefing of messengers before each run. Such a briefing should include up-to-date enemy and friendly troop disposition, alternate routes in emergencies, positive identification of road junctions, and locations of military police or other unit road guards.

(4) Positive marking of legitimate messenger vehicles, which may aid in positive identification and halting by front-line troops in areas short of the front lines.

10. PROTECTION AGAINST TRAFFIC ANALYSIS (T/A)

Traffic analysis (T/A) includes statistical studies of message headings, receipts, acknowledgments, relays, routing instructions, and services; and tabulation of the volume, types and directional flow at each point, with attention to any deviation from the norm or average.

a. To attain a basic understanding of this subject, one should think in terms of --

What does the enemy need to know?

What does the enemy study when he intercepts this traffic?

What use will the enemy make of the resultant intelligence?

The enemy has less interest in the texts of messages (many will be encrypted anyway) than in other parts of the message; namely, the heading and ending. The enemy needs order of battle intelligence which can be obtained from a detailed study of these message parts.

b. For clarity, let's consider radio and wire transmissions only with regard to the extent of intelligence available to traffic analysis, and discuss the feasibility of certain preventive measures.

(1) Fact: Since radio is especially vulnerable to interception, it is therefore vulnerable to traffic analysis.

Theory: Restrict or reduce the use of radio, especially for highly mobile forces, such as armored units.

Application: This theory has limited application, especially for highly mobile forces, such as armored units; it is satisfactory only if alternate means of communications (wire or messenger) are available. As an alternate means, messenger would be unsatisfactory if speed is to be a deciding factor.

(2) Fact: Voice nets are especially vulnerable because of speech characteristics and mannerisms of individual operators (combat leaders and staff officers).

Theory: Rotate operators from one net to another at random intervals, to confuse the enemy and possible thwart his net identification effort.

Application: Impractical -- no commander would entertain such a thought, since voice operators are key leaders and staff officers.

(3) Fact: Violations of procedure aid in unit identification.

Theory: Insist that all users of communications follow the prescribed procedure to the letter, omitting all local expressions and variations in this procedure.

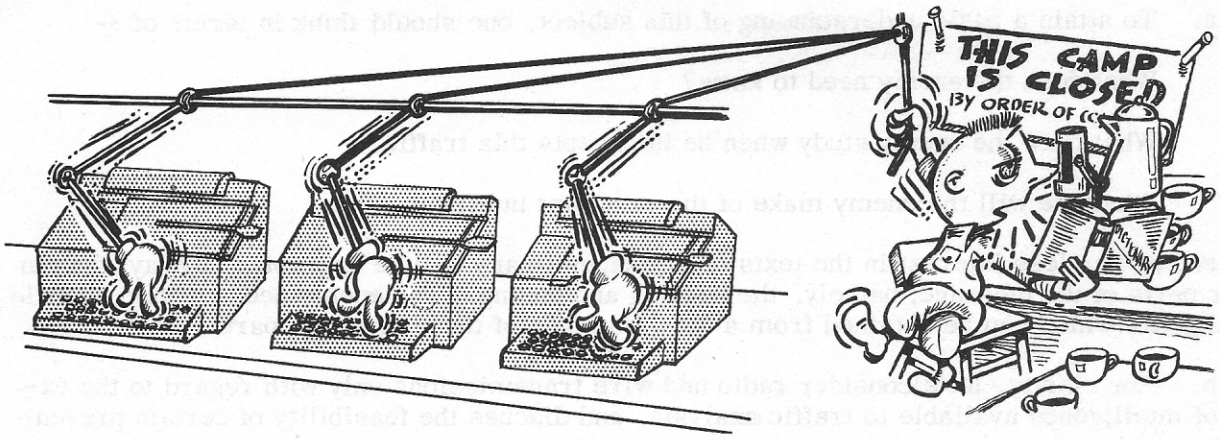
Application: Adherence to the prescribed procedure is the accepted solution to such a problem.

(4) Fact: The enemy obtains information by merely knowing that radios are operating or not operating.

Theory: When the volume of traffic being transmitted drops below normal (average), the commander should order transmission of dummy (false) traffic.

Application: Transmission of dummy traffic is feasible, if thoroughly planned and closely supervised during execution.

(5) Fact: Radio silence, after a prolonger period of radio activity is a "tip-off" of an attack, retrograde action, or change in unit combat assignment.



56002-4

Theory: Do not permit the flow of radio traffic to stop or change materially, until the combat operation has been divulged by other ways to the enemy.

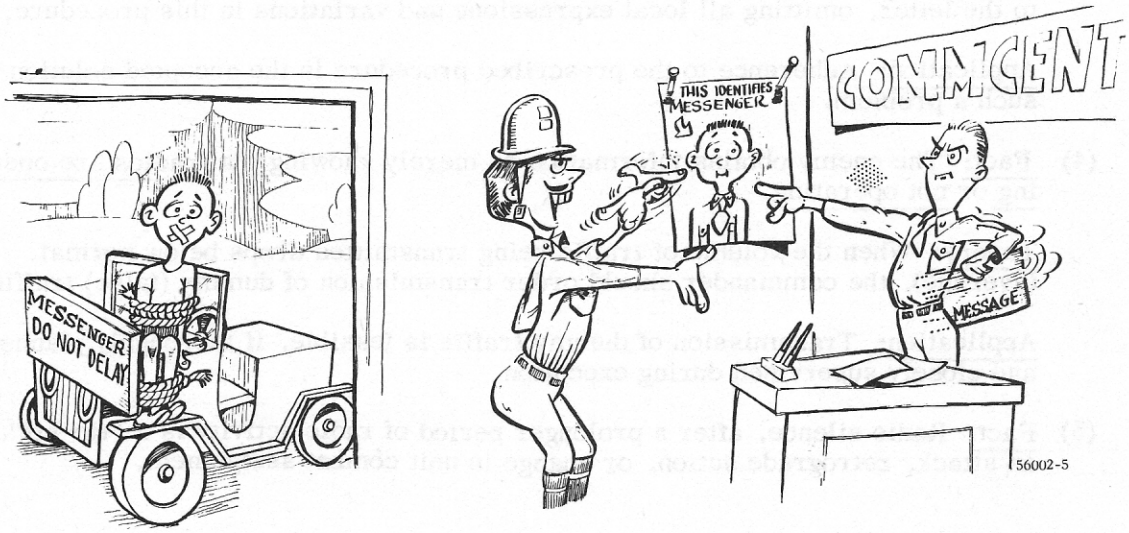
Application: Control of radio traffic flow is feasible and, being a deceptive measure, must be thoroughly planned and closely supervised during execution.

c. Detailed techniques for dummy transmissions and controlled traffic are contained in classified publications under the title, "Communications Deception."

11. PROTECTION AGAINST IMITATIVE DECEPTION

Imitative deception is defined as the introduction of fraudulent transmissions, which imitate authentic transmissions, into communications channels of an opposing force for the purpose of creating confusion, influencing tactical operations, or penetrating communications security. We must assume that the enemy will attempt to deceive us by imitating one of our communication stations or communications personnel. What success will he have?

a. Messenger Service. There is little likelihood that the enemy can successfully impersonate a messenger, since proper messenger operation demands positive identification of all messengers in a particular command. We generally employ messengers in pairs (driver and guard), and are careful to avoid teaming two replacements. Thus we provide continuity of identification and prevent messenger deception. It is imperative to know the messenger or assistant messenger serving your headquarters, signal center or communications center.



56002-5

b. Electrical Circuits. To achieve successful imitative deception against our electrical circuits (radio, wire, or radio-wire) the enemy must be alert to every opportunity. For example:

(1) When one of our radio stations fails to respond to the call of the net control station (NCS), the enemy may elect to imitate that station. His intentions may include receipting for a transmission, thus deceiving the NCS. Should the transmission contain vital information or orders for a subordinate command, it is evident that the successful accomplishment of the mission may be sacrificed as a result of such imitative deception.

COUNTER-COUNTERMEASURE (CCM): This breach of transmission security can ordinarily be prevented by insisting upon authentication under such circumstances. The Standing Signal Instructions (SSI) should contain specific authentication instructions.

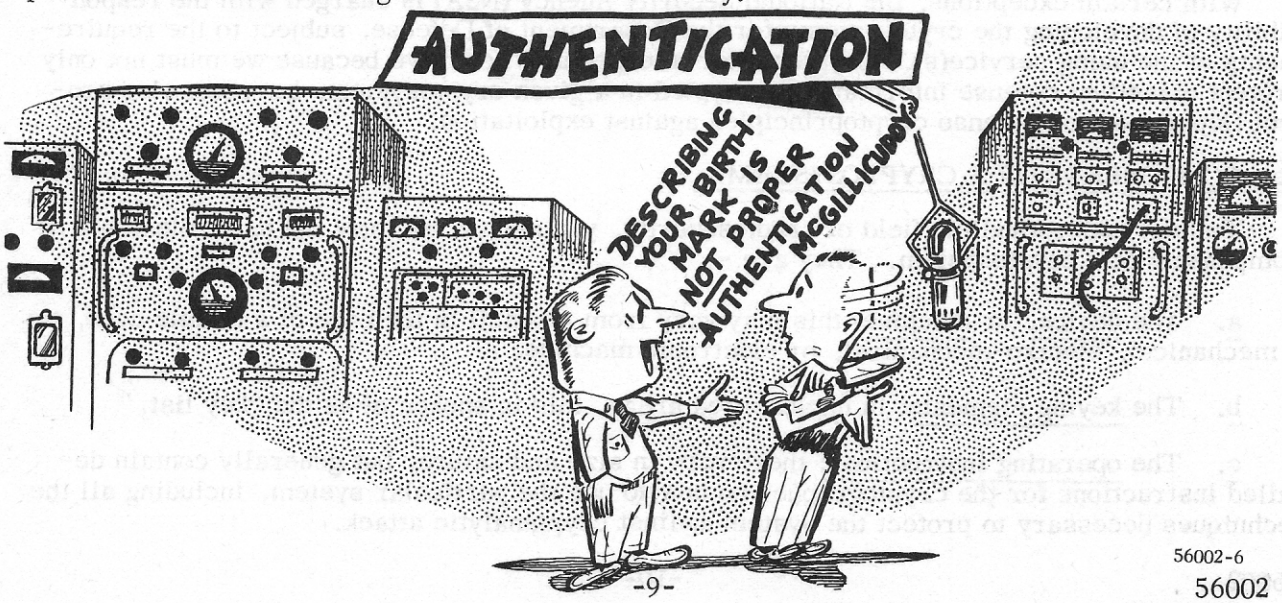
(2) During a period of listening silence (listening watch), the enemy station may imitate one of the stations in the net and transmit a false message to the net control station for the purpose of obtaining a receipt for the transmission. Such an act is intended to reveal the location of the NCS, or obtain some other form of intelligence.

COUNTER-COUNTERMEASURE (CCM): All stations should be alert to this type of imitative deception and should maintain listening silence. If correct transmission authentication doctrine and procedure are followed, this type of deception will prove valueless to the enemy.

12. AUTHENTICATION

Authentication is a communications security measure designed to protect a communications system against fraudulent transmission. Wherever needed, especially at tactical echelons, authentication aids are available in the quantity and type dictated by the commander. Each commander who publishes an SSI and SOI should include adequate authentication tables and instructions for their use.

a. Precautions. Authentication is needed in certain specific circumstances -- for example, the transmission of a tactical message in the clear. This, and many other circumstances where use of authentication is essential, must be included in the command SSI, with specific instructions making authentication mandatory.



56002-6

b. Modes of Operation. Generally speaking, authentication falls into two broad categories:

(1) Challenge and Reply Authentication. By a prearranged procedure described in the unit SSI/SOI, one transmitter (or person) requests authentication of another transmitter (or person) (the challenge) and the latter by proper reply establishes his authenticity (the reply). This technique is most useful when opening or closing a net, or challenging the suspected enemy station.

(2) Transmission Authentication. By a prearranged procedure described in the unit SSI/SOI, a station establishes the authenticity of its own transmission. Such authentication embodies self-authentication, message authentication, and station or net authentication. The authenticator is generally transmitted at the end of a message (transmission), following the operating signal ZNB ("the authentication of this transmission is . . . .").

c. References. Authentication is discussed in the following classified documents which are available to cryptocustodians at division level and above:

KAG-24/TSEC (CLASSIFIED).

AFSAG 1248, Fundamentals of Transmission Security - Joint (U) (CLASSIFIED).

Section III. CRYPTOGRAPHIC SECURITY

13. GENERAL

Cryptographic security results from the development of technically sound cryptosystems, their proper use, and application of proper crypto techniques.

14. BACKGROUND

History is replete with stories of failure due to the weakness of a particular code or cipher. Still other failures resulted from the negligence of a person or persons (cryptographer) using the particular cryptosystem. Cryptographic security (cryptosecurity) must start, therefore, during the developmental stage and must continue through the lifetime of the particular cryptosystem.

15. DEVELOPMENT OF CRYPTOSYSTEMS

With certain exceptions, the National Security Agency (NSA) is charged with the responsibility of developing the crytosystems for the Department of Defense, subject to the requirements of the using service(s). Cryptomatter is especially sensitive because we must not only protect classified defense information encrypted in a given cryptosystem, but must also protect Department of Defense cryptoprinciples against exploitation.

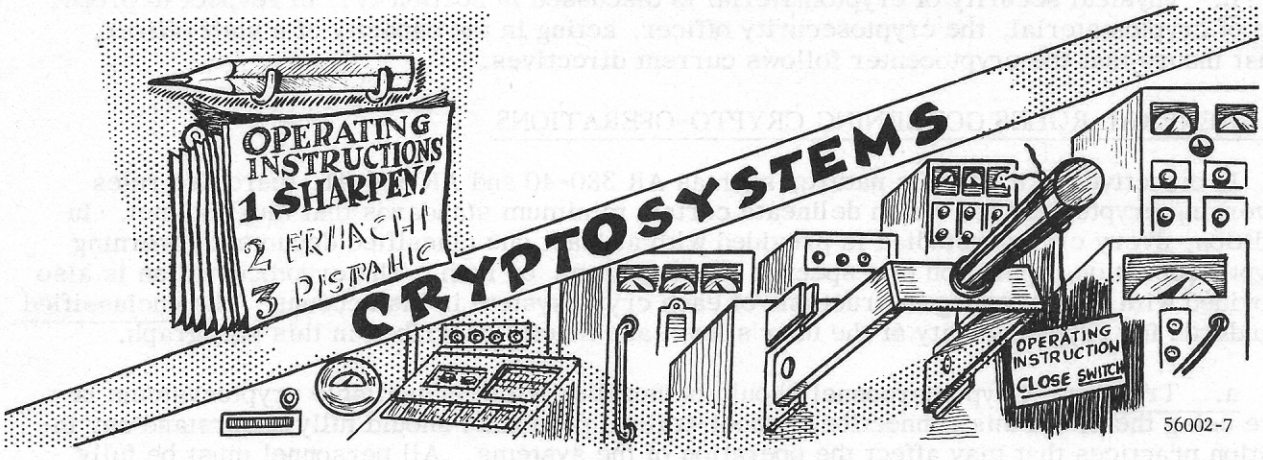
16. COMPONENTS OF A CRYPTOSYSTEM

To fully understand the field of cryptosecurity, you must first know the basic elements or components of a cryptosystem. They are --

a. The device, or machine; this may vary from a pencil in the case of a simple code, to a mechanical, electro-mechanical, or electronic machine.

b. The keying elements; in unclassified areas, this is spoken of as the "key list."

c. The operating instructions; these vary in size and nature, but generally contain detailed instructions for the cryptographer on how to use the particular system, including all the techniques necessary to protect the system against cryptanalytic attack.



17. CLASSES OF CRYPTOMATTER

Cryptomatter falls in three classes, designated as follows:

a. Class 1 Cryptomatter: That cryptomatter, access to which requires a cryptoclearance.

b. Class 2 Cryptomatter: That registered cryptomatter, access to which does not require a cryptoclearance.

c. Class 3 Cryptomatter: That nonregistered cryptomatter, access to which does not require a cryptoclearance.

18. RESPONSIBILITY AT THE USER LEVEL

Before cryptomaterial is issued to a command or agency, proper precautions must be taken in accordance with AR 380-40 and AR 380-41 to insure its proper protection and use upon receipt.

a. The commander will appoint a properly cleared individual as cryptosecurity officer. The cryptosecurity officer is the principal advisor to the commander on all matters pertaining to cryptosecurity and the safeguarding of cryptomatter. When the organization operates a cryptocenter, the cryptosecurity officer will also be responsible to the commander for the secure, accurate, and efficient operation of the cryptocenter. The cryptosecurity officer may also be assigned other duties, such as those of cryptocustodian.

b. Before registered cryptomaterial is issued to an organization, the commander will also appoint an individual on orders to act as cryptocustodian. The person selected will be a properly cleared commissioned or warrant officer, or may be, under exceptional circumstances, a civilian or enlisted person. The cryptocustodian is directly responsible for the physical security of and the proper accounting for all cryptomaterial held by the organization or activity. Other duties, such as those of cryptosecurity officer, or cryptocenter OIC, may be assigned to the cryptocustodian. Most organizations and activities assign one person to perform the duties of cryptosecurity officer and cryptocustodian.

c. A properly cleared person (assignment criteria are the same as for custodian) will be appointed on orders to act as alternate cryptocustodian, for the purpose of providing continuity of responsibility for the physical security of, and the proper accounting for, all cryptomaterial held by an organization or activity during the absence of the cryptocustodian. To further insure continuity, more than one alternate cryptocustodian may be appointed.

d. Physical security of cryptomaterial is discussed in Section IV. In respect to proper use of cryptomaterial, the cryptosecurity officer, acting in the capacity of a staff officer, must insure that the cryptocenter follows current directives.

19. GENERAL RULES GOVERNING CRYPTO-OPERATIONS

In directives of a specific nature, such as AR 380-40 and AR 380-41, there are rules governing cryptofacilities which delineate certain minimum standards that must be met. In addition, every cryptocustodian is provided with at least one classified document governing crypto-operation, operation of a specific cryptosystem, or both. The cryptocustodian is also provided with the operating instructions of each cryptosystem in his account. The unclassified standards for cryptosecurity at the user's level are briefly described in this paragraph.

a. Training. Cryptopersonnel should be familiar with the available cryptosystems before using them. In this connection, school-trained personnel should fully understand any in-station practices that may affect the operation of the systems. All personnel must be fully acquainted with any changes to the system.

b. Supervision. A qualified person must supervise encryption and decryption. This requirement is normally met by having the cryptosecurity officer, or someone designated by him, physically present in the cryptocenter when it is in operation. In any event, the supervisor should possess the security clearance equal to the highest classification of traffic that can reasonably be expected.

c. Check-Decryption of All Outgoing Messages. This is the process of ensuring that the message is properly encrypted by decrypting it before transmission.

d. Paraphrasing. Paraphrasing is the process of rewriting a message so that the meaning is the same but the phraseology is different and the contents rearranged.

(1) Responsibility. Both the originator and the addressee are responsible for determining the need for paraphrase of messages. The cryptosecurity officer will assist in determining those messages or portions of messages which require paraphrasing.

(2) Method. Except when paraphrase is required for only a portion of the text, such as a classified extract in an otherwise unclassified message, apply the following process to the entire message:

(a) Change the sequence of paragraphs and sentences.

(b) Shift the positions of the subject, predicate, and modifiers in the sentences.

(c) Substitute synonyms or equivalent expressions.

(3) Classification. Paraphrase is only a cryptographic safeguard and does not alter the classification of the message.

20. SPECIFIC RULES GOVERNING CRYPTO-OPERATION

In addition to directives such as AR 380-40, each specific cryptosystem is governed by a set of operating instructions. This set of instructions constitutes a major portion of any system. It comprises a set of rules and techniques to guide the cryptographer in the one correct way of using the system. To accomplish the purpose of preventing or delaying cryptanalysis, therefore, the user must follow every rule, step, or process in painstaking detail. While it is essential to preserve a common sense attitude toward security, it is equally essential to recognize the

special sensitivity of cryptomatter. Attainment of the desired balance between security and operational effectiveness requires intelligent direction by those in responsible positions and constant vigilance in the performance of duty by all subordinates.

Section IV. PHYSICAL SECURITY

21. GENERAL

Physical security results from all measures designed to protect classified communications equipment and material from access thereto by unauthorized persons.

22. RESPONSIBILITY FOR SAFEGUARD

Direct responsibility for safeguarding classified cryptomatter rests upon both the commander and the individual who is in a physical position to exercise direct security control -- the cryptocustodian.

23. INITIAL ISSUE OF CRYPTOMATERIAL

Each prospective user of cryptomaterial must consult his local signal officer to determine the type of cryptomaterial required and the method of requisitioning. The signal officer will verify the requirement, based upon the mission of the unit or agency, and will contact the distribution authority responsible for such cryptologistic support. Thereafter, the prospective user must meet specified security requirements before and after distribution of the cryptomaterial.

24. PHYSICAL SECURITY CRITERIA PRIOR TO ISSUE OF CRYPTOMATERIAL

Acting for the commander, the cryptosecurity officer must provide the following safeguards before cryptomaterial is issued to his organization or activity:

a. Structural Strength/Armed Guard. The cryptofacility must possess sufficient structural strength to prevent forceful entry, or armed guards as a substitute.

b. Screening from View. The area selected for crypto-operations must be screened to prevent comprehensive viewing of material and operations.

c. Soundproofing. The cryptofacility must be reasonably soundproof. There can be no hard and fast rules on soundproofing; instead, the cryptosecurity officer must be guided by the location and type of structure and the sensitivity of the cryptomaterial used or stored in it. Soundproofing may give a cryptosecurity officer a false sense of security.

d. Clearances.

(1) Cryptopersonnel. Individuals selected for cryptoduties must meet the following criteria:

(a) Security clearances (TOP SECRET, SECRET, CONFIDENTIAL) must be equal to the highest classification of information each individual will have access to. The cryptosecurity officer must determine, by consulting the command, the highest security classification of traffic (messages) that can reasonably be expected in the cryptocenter.

(b) Cryptologic clearance must be obtained for all persons whose duties involve access to cryptomatter requiring cryptoclearance (class 1 cryptomatter), or whose assignment is to a crypto-area in which such matter is held.

(2) The commander. If the organization possesses critical material, the commander should be issued a cryptologic clearance in addition to a security clearance for other than critical material. This is not a requirement by regulation, but it is a sensible approach to keeping the commander informed. It will also better enable the commander to meet the requirements of the regulation that places responsibility for safeguard on him and on the cryptocustodian. This matter is further discussed in paragraphs 28 and 29 on inspections.

e. Safes/Vaults. Security for classified cryptomatter is provided either by a vault with a three-position dial-type combination lock, or by a safe or file cabinet equipped with a three-position dial-type combination lock, the container being of sufficient size and weight to make the possibility of its physical removal negligible. Additional physical safeguards are required for certain items of class 1 cryptomaterial as indicated in the cryptopublication, KAG-1( )/TSEC. An additional safeguard for all types of cryptomaterial requires that, so far as practicable, classified keying material will NOT be stored in the same container with associated devices, machines, or operating instructions, unless in a vault which is used only for the storage of cryptomaterial.

25. ACCOUNTABILITY FOR CLASSIFIED CRYPTOMATERIAL

To fully appreciate the impact of cryptographic accountability, it is well to recall that physical security rests upon both the commander and the cryptocustodian. The cryptocustodian is required to acknowledge receipt of all cryptomaterial by transfer report (DA Form 223). This places a personal burden upon him and invites his vigilant attention to such an important duty; anything less than his best duty borders on negligence. Accountability for cryptomaterial includes certain rules, normally inflexible. The regulations (principally AR 380-40 and AR 380-41) are amended or waived only in exceptional circumstances, and then only with the explicit approval of the Chief, U. S. Army Security Agency (USASA). The gist of accounting criteria follows:

a. Change of Custodian. Anticipated change in custodians is reported to the office of issue at least 7 days in advance of any transfer of cryptomaterial if reporting by message, and at least 10 days in advance if reporting by letter. The transfer must be accomplished by a joint physical inventory.

b. Temporary Absence of Custodian. The requirements for transfer of cryptomaterial during a temporary absence of the custodian differ according to the duration of the absence.

(1) Less than 72 hours. The alternate custodian will receipt for packages, open them, and verify the contents.

(2) Less than 4 weeks but more than 72 hours. The alternate custodian will have transferred to him and reported to the office of issue all current material, material scheduled for destruction, material scheduled for use, or material scheduled for some other action such as return to office of issue. All other material (reserve) will be kept in separate, secure storage and will not be transferred unless the quarterly inventory falls due during the period. Should the inventory fall due, all material is transferred to the alternate custodian, who will assume the duties of the cryptocustodian. Another individual must then be appointed as alternate cryptocustodian.

(3) More than 4 weeks. If the custodian is to be absent more than four weeks, all material must be transferred and reported to the office of issue. The person accepting responsibility becomes the cryptocustodian. Upon return of the regular cryptocustodian, a complete transfer is made of all material. All additions, destructions, and similar actions will be reconciled.

c. Quarterly Inventory. On the last day of each quarter (31 March, 30 June, 30 September, and 31 December), an inventory of all accountable cryptomaterial will be made by the cryptocustodian and a witnessing officer, and a report (DA Form 223) will be rendered to the office of issue.

d. Daily Security Check. Regulations require the following daily security checks:

(1) Inventory of cryptomaterial. At the end of each workday or between shifts, as appropriate, an inventory of class 1 and 2 cryptomaterial will be made. Reserve, obsolete, and future cryptomaterial, when kept in separate storage, need not be inventoried. A record will be maintained indicating the short title of each item inventoried, the initials of the person making the inventory, and the time that the inventory was made. Daily inventory records will be retained until the next quarterly inventory, after which they may be destroyed. These provisions do not apply to offices of record and issue.

(2) Safe, cabinet, or area check. At the end of each workday, except in cryptofacilities operating on a 24-hour basis, a security check will be made of all safes and cabinets or entrances to secure cryptofacilities containing class 1 or 2 cryptomaterial. DA Form 672 (Safe or Cabinet Security Record) is prescribed by AR 380-5 for this purpose. In facilities holding class 1 cryptomaterial, unless all cryptomaterial is stored in a vault or secure room or is protected by an armed guard to the extent that the possibility of undetected access is negligible, an additional check will be made each non-workday to insure that all locking devices are secured. The non-workday check will be made by cryptopersonnel or by specifically designated personnel of undoubted loyalty.

26. ACCESS TO CRYPTOFACILITY

a. Authorized Access List. Each cryptofacility devoted to the operation or storage of class 1 cryptomatter (and class 2 cryptomatter at the commander's discretion) will maintain a current list of personnel assigned or authorized access to the facility. The list will be authenticated by the commander or his authorized representative and posted inside the cryptofacility near the entrance; in the case of an administrative crypto-account, the list will be filed adjacent to the crypto-documents. (An administrative crypto-account is one that is established for holders of cryptodocuments to be used for reference only, and not for operations.)

b. Visitor Register. Persons other than those whose names appear on the authorized access list will not be permitted to enter cryptofacilities except with the approval of the commander or his authorized representative. DA Form 1999 (Crypto-Area Visitor Register) will be maintained to record the arrival and departure of such visitors. This provision does not apply to administrative crypto-accounts.

c. Uncleared Personnel. When uncleared personnel are admitted to the cryptofacility, the following additional stringent precautions will be taken:

(1) All classified cryptomaterial will be protected from viewing, and the uncleared person will be denied any other source of classified crypto-information. Cleared personnel will keep uncleared personnel under constant surveillance during the entire period they are in the area.

(2) When the commander considers it necessary for an uncleared person to inspect the facility, or to inventory or witness the destruction of cryptomaterial, only the cover pages of documents and the nameplates of crypto-equipment will be viewed.

27. DISPOSITION OF CRYPTOMATERIAL

a. Routine Destruction. As cryptomaterial becomes superseded through normal or directed supersession, the cryptocustodian must make adequate provisions for routine destruction. Since cryptomaterial has a special sensitivity, extreme care must be taken to insure that destruction is complete, whatever the method used. There are no hard and fast rules concerning the advisability of a separate incinerator for the cryptoactivity. Each organization or activity must treat this subject as an in-station problem.

b. Emergency Destruction Plan. Each cryptofacility must have a current plan for the swift and systematic destruction of all classified cryptomaterial in the event of its possible, or probable, capture or abandonment. Normally such a plan is implemented on the order of the commander or his authorized representative. The plan must provide, however, for the delegation of this authority to the senior person in the cryptofacility whenever the urgency of the situation requires an on-the-spot decision. The plan should undergo dry-runs periodically. The manner and priority of destruction is specified in the various effective cryptopublications. Familiarity with these references eliminates any false sense of values concerning priority of destruction.

c. Emergency Evacuation Plan. Each cryptofacility must also have a current plan for the evacuation of cryptomaterial in the event of an emergency, such as hostile action. The plan must be fully coordinated, since its success may often depend upon assistance from sources other than the cryptofacility, and it should be in sufficient detail so that the senior person present can implement it promptly and successfully.

d. Disaster Plans. Each cryptofacility must, in addition to the evacuation and destruction plans, carefully consider the actions to be taken under threat of fire, flood, hurricane, and other calamities which would endanger life, government property, and the security of cryptomaterial. Such plans must provide for maximum security during and after such a calamity and should include provisions for evacuation and/or destruction in the face of inadequate security. It is well to remember that cryptomaterial can be replaced if destroyed, but security when lost can never be regained.

28. COMMAND INSPECTIONS

a. General. The commander is responsible for making, or causing to be made by an officer of his command, thorough inspections to insure that cryptomaterial is used, stored, distributed and accounted for, and crypto-equipment maintained, in accordance with Department of Defense and Department of the Army directives.

b. Frequency of Inspections. The major commander prescribes the frequency of crypto-inspections within the command; these inspections are in addition to those prescribed by USASA. Command inspections should be spaced throughout the year to insure that all security measures and directives pertaining to crypto-operations are being strictly observed, that newly assigned personnel are brought under surveillance, and that changing methods of operation and fluctuations in the scope or nature of cryptoactivities are adequately covered.

c. Selection of Inspectors. In order not to endanger security, the person selected to perform the command inspection must be cleared for access to the highest security classification and type of material to be viewed and should be a person other than one assigned to the cryptofacility to be inspected. (This does not prevent the signal officer or the cryptosecurity officer from performing the command inspection of subordinate commands.)

d. Record of Command Inspections. The cryptosecurity officer of each command maintains a record of all command inspections in compliance with AR 380-40, AR 380-46, and AR 750-8. Such records include date of inspection, brief description of findings, recommendations, and corrective action taken, as applicable. (These records should prove useful to future commanders and cryptosecurity officers in determining the "trends" of the cryptofacility. The USASA representative, during his inspections, also reviews all such records.)

29. USASA INSPECTIONS

a. General. The U. S. Army Security Agency is responsible for the technical supervision of communications security activities of the U. S. Army and of civilian organizations receiving cryptosupport from the Army. In discharging its responsibilities, USASA conducts inspections of cryptofacilities to insure that cryptomaterial is used, stored, distributed and accounted for, and crypto-equipment maintained, in accordance with current directives. Such inspections are made annually and at such other times as the Chief, USASA, directs.

b. Action Prior to Inspection. On notification of a forthcoming USASA inspection, the commander will prepare a statement verifying the name, grade, and type of clearance held by each person on the authorized access list.

c. Conducting Inspections. Inspections are conducted in accordance with procedures established by the Chief, USASA. Each inspection will include a spot check of accountable cryptomaterial and, when applicable, an examination of crypto-operations, physical security measures, state of training of cryptopersonnel, crypto-equipment maintenance procedures, and a review of the record of command inspections.

Section V. ATTAINMENT OF COMMUNICATIONS SECURITY

30. GENERAL

a. Each commander is responsible for the success or failure of communications security within his command. In order to have a successful COMSEC program, he should fully utilize the services of his staff advisor on such matters -- the signal/communications officer. In turn, the signal/communications officer should be responsible for the planning, coordination and supervision of all COMSEC matters within the command.

b. COMSEC can best be regarded as a field of endeavor which must be fully integrated with all operational matters within the command and upon which may rest the success or failure of the mission. This section summarizes certain processes by the commander and his delegated representative which must be followed in painstaking detail in order to bring the state of training up to desirable standards.

31. INDOCTRINATION OF ALL USERS OF SIGNAL COMMUNICATIONS AND CRYPTOMATTER

This area involves careful briefing of all interested staff members and operating personnel concerning capabilities and limitations of their communications equipment and cryptomatter, procedures prescribed for their use, susceptibility of the communications system to interception and imitative deception, vulnerability of specific cryptomatter, and ways by which each individual can help provide the communications security so vital to all commands. A well-informed individual is in a better position to help than is an ill-informed one.

32. TRAINING ALL USERS OF SIGNAL COMMUNICATIONS AND CRYPTOMATTER

To permit untrained troops access to and use of communications equipment and cryptomatter would be just as foolhardy as to permit untrained or ill-trained personnel to operate motor vehicles or weapons. The results would be comparable and would undoubtedly contribute to the ultimate failure of the command's mission. Certain minimum standards of training should be announced to all communications users.

33. SUPERVISORY EFFORTS AT ALL LEVELS OF COMMAND

Proper supervision and immediate remedial action for all violations of regulations and procedures are necessary if the command expects to reach combat efficiency. As in all other fields of endeavor, the commanders and their respective communication officers must take aggressive supervisory action. Such supervision includes maintenance as well as operations.

34. NET CONTROL OF RADIO NETS

This is especially important throughout all phases of operations. Adherence by all personnel to the prescribed procedure will aid in preventing confusion, enemy deception, and loss of net operating time.

35. AUTHENTICATION

Since authentication is a safeguard against imitative deception, it is imperative that all authentication techniques and procedures be followed exactly. Also, since authentication tables and techniques are a form of cryptomatter, proper security precautions must be adhered to.

36. MONITORING

To ensure that all personnel are using communications equipment properly, including correct procedures, each commander is responsible for the monitoring of his circuits. No other agency is charged with this function.

37. COMMUNICATIONS ANALYSIS

This is the process of analyzing one's own communications for the purpose of determining its security status. During the conduct of such analyses, the commander will insure that specified circuits are monitored, violations analyzed, and the results disseminated to affected units or individuals. It is believed that security violations will be greatly reduced if the command knows a monitoring program is in effect.

APPENDIX I. COMMUNICATIONS SECURITY REFERENCES

ACP 122( )	Communications Instructions -- Security (U) (CLASSIFIED)
ACP 165	CLASSIFIED
ACP 256	CLASSIFIED
ACP 257	CLASSIFIED
AFSAG 1248	Fundamentals of Transmission Security - Joint (U) (CLASSIFIED)
AR 105-31	Message Preparation
AR 105-40	Teletypewriter Conferences
AR 345-274	Records Administration -- Maintenance and Disposition of Intelligence and Security Administration Files
AR 380-5	Military Security -- Safeguarding Defense Information
AR 380-20	Military Security -- Restricted Areas
AR 380-40	Military Security -- Safeguarding Cryptomatter
AR 380-41	Military Security -- Control of Cryptomaterial
AR 380-46	Military Security -- Radiation of Intelligence-Bearing Information by Communications, Communications Security and Duplicating Equipments (U) (CLASSIFIED)
AR 380-105	Military Security -- Policy and Procedure Governing Use of Code Words, Nicknames, Short Titles and Similar Devices
AR 604-5	Personnel Security Clearance -- Investigation and Clearance of Personnel for Handling Cryptologic, Top Secret, Secret and Confidential Material and Information
COMLOG-1( )	CLASSIFIED
COMSEP-1	CLASSIFIED
DA MEMO 105-5	Communications -- Army Communications-Electronic Objectives (U) (CLASSIFIED)
FM 32-5	Communications Security (U) (CLASSIFIED)
KAG-1( )/TSEC	CLASSIFIED
KAG-21/TSEC	CLASSIFIED
KAG-24/TSEC	CLASSIFIED
TB 105-1	Communications Security (U) (CLASSIFIED)
TB 105-2	Communications Security (U) (CLASSIFIED)
TB 380-1	Communications Security -- The Plain Language Dilemma (U) (CLASSIFIED)

CONTENTS

Army-Ft Monmouth,NJ-MON 3341-60