

CHAPTER 7 COMMUNICATIONS

Section I. General

ASSETS AND SERVICES

Communications help you support unit missions, carry out administrative duties, maintain contact with higher headquarters, transmit tactical information, and defend the unit. The commander must set up communications with all elements. Their personnel must communicate with higher headquarters, supported units, and internal elements. Communications help may be needed in setting up an adequate system. Assistance can usually be obtained from COSCOM or EAC in which the unit may operate, from the battalion headquarters company to the subordinate units, or from the headquarters detachment of a petroleum group.

Assets

Communications equipment authorized includes the AN/GRC-106/160/193, AN/PRC-77, AN/VRC-43/46/47, VRC-87/88/89/90/91/92 series radios, AN/VRC-97 MSE, and the AN/GRA-6/39 radio set control groups. See Appendix B for a complete equipment listing and publication data. The commander is responsible for allocating these communications assets. Equipment should be allocated as needed to perform the mission. For example, in a tactical situation, OPs or LPs might have priority on phones. Another source of communications would be the MP security company, if attached to the petroleum group. It would have organic communications equipment mounted on each of its vehicles.

Services

Communications services will differ depending on the area or zone in which the unit operates. Services are provided in both the COMMZ and the corps area.

In the COMMZ. Because the unit will be deployed throughout the COMMZ, you will need outside help to set up your communications system. This assistance comes from signal organizations of the communications command in EAC. These signal units install, operate, and maintain a network of area signal centers in the COMMZ. Trunking systems connect the centers. Use the centers to supplement your organic communications to higher, subordinate, or nearby units.

In the corps. The corps communications system operates in the combat zone and provides communications for corps units. It is an integrated system with a single-channel command radio and multichannel facilities to provide service on both command and area basis. Direct links go from corps main command post to assigned divisions and selected subordinate units. The area communications system is linked to the command system. The area system has area signal centers (nodes) situated to provide corps-wide access. The corps system is linked to the communications system of the EAC and to adjacent corps and divisions.

METHODS

There are many different communication methods. Use the methods that offer maximum reliability, flexibility, security, and speed with a minimum of effort and material. Do not depend on one method. Use methods which complement each other. Also, signal equipment (particularly when connected to cables or antennas) can be damaged by electromagnetic pulse. Alternate means of communication should always be available in the event of nuclear warfare. Refer to FM 24-1 for more information on the various methods of communication.

Wire and cable

Wire systems use field wire and cable, telephones, and the switchboard to provide person-to-person conversations. Wire is more secure than radio. If radio links are used in your system, the enemy can intercept your telephone conversations. Make sure your personnel know this and practice communications security. Be sure to cover security in the unit SOP. In your SOP, include details of the telephone system, priorities for laying wire, and responsibilities for setting up the system. See FM 24-20 for information on field wire activities and the general characteristics of equipment used with field wire systems.

Radio

Make sure the allocation of radio equipment is documented in the SOP. Radio is one of the most versatile methods of communication. Since it is wireless, you can operate while mobile. It can handle large volumes of traffic. Radio is your main method of communication with unit elements too far away for contact by local telephone. However, radio is the least secure communications method. Radio communication is subject to jamming and interception, deception, and interference. Radios can be severely damaged by the electromagnetic pulse resulting from a nuclear detonation. During the blackout (ionization of the atmosphere) following detonation, radio transmissions will be impossible. If your unit is in or expects to be in a nuclear environment, measures must be taken to protect your radios. For more information, refer to FM 25-50. Put both security and protective measures in your unit SOP. When setting up operating sites, your personnel should enter the net using procedures in FM 24-18.

Automation

Automation means are methods of sending, receiving, processing, or storing information by an automated capability (such as computers). Automated capability is able to process large volumes of information and provide real-time delivery. Automation provides speed, accuracy, improved text and video display, programmable output and formats, and is easily secured. However, it requires a manual system for a backup and is susceptible to electromagnetic pulse, power fluctuations, induced viruses and magnetic disturbances.

Manual

Manual method consists of sending, receiving, or storing documents by physical capabilities, without passing over electronic media. This method includes messengers and records management system. This method is reliable, flexible, and uses assets found in every unit. It is also the most secure means available. The records management system provides a backup for data storage. However, there is a large requirement for space. It is manpower intensive. The messenger, when used, is subject to enemy intervention and may be constrained by weather, terrain, and time.

Visual and sound signals

Visual and sound signals can be used to send messages over short distances. These signals are most useful during periods of radio silence. They are used as alarms or warnings, especially of enemy attack, or as a means of sending prearranged messages. Messages transmitted by visual or sound signal are easily misunderstood; therefore, care must be taken in the selection of the means and the message to be conveyed. Messages transmitted by this means should be few, prearranged, and simple. Visual signals include road signs, flags, lights, panels, arm and hand signals, and pyrotechnics. Sound signals include horns, bells, whistles, weapons fire, and sirens.

Section II. Defense Against Electronic Warfare

SECURITY

COMSEC consists of measures taken to keep unauthorized persons from getting information from the communications system. Make sure your personnel understand and observe COMSEC measures described in AR 380-40. Two measures they should practice are transmission security and physical security.

Transmission Security

All transmissions are governed by the SOI. SOI is a series of orders issued for technical control and coordination of signal support activities for a command. As a rule, you receive only an extract of a SOI, that part necessary to manage your nets. Among other things, the SOI may give you a list of EEFI which must not be transmitted. Your operators will have a copy of this list. They should monitor transmissions to see if information on the list is being passed. Other ways for making transmissions more secure are:

- Choose means of communication according to the urgency of the situation. Use the most secure means to send your message.
- Transmit only when necessary.
- Use low transmitting power when possible.
- Be wary if a radio station's signal strength suddenly changes.
- Plan your message. Keep the message as short as possible.
- Cut out unnecessary talk. Maintain communication silence as much as possible.
- Use only authorized codes and ciphers.
- Avoid identifying yourself or others.
- Demand authentication. Do not talk to anyone who will not authenticate.

Physical Security

Impress on your operators the need to protect communications equipment from abuse, damage, or capture. Make sure they guard against disclosing the locations of equipment. Phone wires should be put inside the defensive perimeter and along frequently traveled routes. Bury wires and cables whenever possible to protect against electromagnetic pulse. Proper grounding will also protect electronic equipment during nuclear attack. Radios should be put in well defended locations. Instruct your operators to move transmitters frequently. Be sure to rotate your operators so that an enemy will not associate an operator with a specific unit or operation.

UNWANTED SIGNALS

Radio reception may be hindered, confused, or prevented by unwanted signals. These signals may be unintentional (from friendly or natural sources) or intentional (from unfriendly sources). Unwanted signals should be reported according to SOI supplemental instructions. Before reporting, the operator should disconnect the receiving antenna to determine whether or not the unwanted signal is from an outside source. The operator should follow the procedures in FM 24-33 to determine the nature of the unwanted signal.

Unintentional Signals

Electromagnetic signals caused by sources other than the enemy may interfere with your radio reception. These sources include friendly radio signals, faulty electrical components, weather conditions, and nearby generators. This type of unwanted signal is caused interference.

Intentional Signals

Electronic devices have created ways for the enemy to operate against you in combat situations. Through electronic warfare, the enemy attempts to monitor and break up your communications. The intentional unwanted signals you will most often encounter include deception, jamming, and squelch capture.

Deception. Deception is the entrance of false or altered information into friendly signal paths so that operators react to it. The enemy may try to enter the communications system by imitating a friendly unit or station so as to get or give information that could affect an operation. Train your operators to counter deception by using correct operation codes, brevity lists, and operating signals. Make certain they require authentication and observe transmission security.

Jamming. Jamming is the deliberate effort to prevent the passage of information or degrade reception. It can disrupt a single frequency or a frequency spectrum. All radio frequencies can be jammed. An operator who hears an unusual noise on the radio must try to determine its source. If it cannot be traced to a friendly source, the radio is probably being jammed. The operator should try to identify the kind of noise and report it. Under no circumstances, should the operator let the enemy know that jamming efforts are successful. Antijamming measures and techniques are described in FM 24-33.

Reports

When an operator suspects interference, you should be notified immediately. The operator should make a report according to SOI supplemental instructions and in the format shown in FM 24-1. The report should be made whether or not the operator is successful in working through the interference. After you review the report, send it to higher headquarters. This is required by the SOI.