ATP 6-02.46

EXPEDITIONARY SIGNAL COMPANIES

MAY 2025

DISTRIBUTION RESTRICTION: Approved for public release, distribution is unlimited.

HEADQUARTERS, DEPARTMENT OF THE ARMY

This publication is available at the Army Publishing Directorate Website (https://armypubs.army.mil) and the Central Army Registry Website (https://atiam.train.army.mil/catalog/dashboard).

Army Techniques Publication
No. 6-02.46

Headquarters
Department of the Army
Washington, DC, 07 May 2025

EXPEDITIONARY SIGNAL COMPANIES

Contents

Page

Preface ..... **v**
Introduction ..... **vii**
CHAPTER 1 ..... **1**
OPERATIONAL ENVIRONMENT AND THREAT **1**
Understanding the Environment 1
Threats 2
CHAPTER 2 ..... **5**
ORGANIZATION OF SIGNAL SUPPORT ELEMENTS **5**
Unit Organization 5
Roles and Responsibilities 27
CHAPTER 3 ..... **37**
PLANNING IN THE COMPANY **37**
Section I – The Operations Process **37**
Planning 37
Preparation 38
Execution 39
Assessment 39
Section II – Planning Considerations **40**
Deployment and Employment of Units 40

DISTRIBUTION RESTRICTION: Approved for public, distribution is unlimited.

Unique Planning Requirements 41
Section III – Troop Leading Procedures 48
Step 1 – Receive the Mission 49
Step 2 – Issue a Warning Order 49
Step 3 – Make a Tentative Plan 51
Step 4 – Initiate Movement 66
Step 5 – Conduct Reconnaissance 66
Step 6 – Complete the Plan 66
Step 7 – Issue the Order 67
Step 8 – Supervise and Refine 68
Abbreviated Troop Leading Procedures 69
Section IV – Rehearsals 69
Rehearsal Purposes 70
Rehearsal Types 70
Methods of Rehearsals 72
Pre-combat Checks and Inspections 73
Section V – Recovery 75
Recovery 75
CHAPTER 4 77
SUPPORT TO OPERATIONS 77
Reception, Staging, Onward Movement, and Integration 77
Command Post Support 77
Organizations Requiring Tactical Communications Augmentation 83
Homeland Defense, Homeland Security, and Humanitarian Assistance 84
Command and Support Relationships 87
CHAPTER 5 89
LOGISTICS AND SUSTAINMENT 89
Section I – Maintenance 89
Maintenance Management 89
Two-Level Maintenance 90
Communications-Electronics Maintenance 95
Section II – Supply 96
Resupply 97

CHAPTER 6 103
UNIT TRAINING 103
Section I – Training in the Company 103
Collective Training Techniques 103
Realistic Training Environment 104
Digital Battle Drills 104
Combined Arms Training Strategy 104
8-Step Training Model 106
Safety 110
Section II – Signal Assessment Tables 114
Table I – Individual Training 114
Table II – Individual Skills Test 117
Table III – Team Training 118
Table IV – Team Certification 121
Table V – Section Training 124
Table VI – Section Certification 126
Table VII – Section Validation 129
APPENDIX A 135
RECOGNIZING AND RESPONDING TO CYBER AND ELECTROMAGNETIC WARFARE ATTACKS 135
Glossary 151
References 157
Index 161

Figures

Figure 2-1. Expeditionary signal battalion organization chart 6
Figure 2-2. Expeditionary signal company organization chart 8
Figure 2-3. Joint and area signal company organizational chart 12
Figure 2-4. Expeditionary signal battalion-enhanced organization chart 18
Figure 2-5. Expeditionary signal company-enhanced organization chart 20
Figure 2-6. Enroute communications company organization chart 25
Figure 3-1. Parallel sequences of the military decision-making process and troop leading procedures 38
Figure 3-2. Example warning order format 50
Figure 3-3. Commander's critical information requirements 58

Figure 3-4. Operation order format 68
Figure 3-5. Methods of rehearsals 72
Figure 5-1. Tailgate resupply 99
Figure 5-2. Service station resupply 100
Figure 6-1. The 8-step training model 106
Figure 6-2. Training variable assessment table 109
Figure 6-3. Signal assessment tables I–IV 124
Figure 6-4. Signal assessment tables V–VII 133

Tables

Table 2-1. Equipment allocations in the joint and area signal company 14
Table 2-2. Equipment allocations in the expeditionary signal company-enhanced 22
Table 2-3. Equipment allocations in the enroute communications company 26
Table 4-1. Emission control conditions 82
Table 5-1. Alignment of units to type of maintenance performed 95
Table 5-2. Classes of supply 97
Table 6-1. Work-rest cycles and water consumption 112
Table A-1. Common jamming signals 139

Preface

ATP 6-02.46 provides doctrinal guidance for leaders responsible for planning, preparing, executing, and assessing operations of expeditionary signal companies. This publication serves as an authoritative reference for personnel developing doctrine, materiel, and force structure; institutional and unit training; and standard operating procedures. For this manual, 'expeditionary signal companies' includes the—

- Expeditionary signal company.
- Expeditionary signal company-enhanced.
- Joint and area signal company.
- En route communications company.

The doctrinal principles and techniques contained in this publication are intended to be used as a guide and are not prescriptive. To properly apply this doctrine, readers must be familiar with ADP 3-0, FM 3-0, FM 6-02, and ATP 6-02.45.

The principal audience for ATP 6-02.46 is leaders and signal Soldiers in expeditionary signal companies. Commanders and staffs of Army headquarters serving as joint task force or multinational headquarters should also refer to applicable joint or multinational doctrine concerning the range of military operations and joint or multinational forces. Trainers and educators throughout the Army will also use this publication.

Commanders, staffs, and subordinates must ensure that their decisions and actions comply with applicable U.S., international, and in some cases host-nation laws and regulations. Commanders at all levels will ensure that their Soldiers operate in accordance with the law of armed conflict and applicable rules of engagement (see FM 6-27). They also adhere to the Army Ethic as described in ADP 6-22.

ATP 6-02.46 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. This publication is not the proponent for any Army terms. For other definitions shown in the text, the term is italicized, and the number of the proponent publication follows the definition.

ATP 6-02.46 applies to the Active Army, Army National Guard/Army National Guard of the United States, and United States Army Reserve unless otherwise stated.

The proponent of ATP 6-02.46 is the United States Army Cyber Center of Excellence. The preparing agency is the Doctrine Branch, United States Army Cyber Center of Excellence. Send comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Commander, United States Army Cyber Center of Excellence and Fort Gordon, ATTN: ATZH-OPD (ATP 6-02.46), 419 B Street, Fort Gordon, GA 30905-5735; by e-mail to usarmy.gordon.cyber-coe.mbx.gord-fg-doctrine@army.mil.

This page intentionally left blank.

Introduction

ATP 6-02.46 provides techniques for expeditionary signal companies at echelons above corps and in the corps signal brigade. This publication provides doctrinal guidance; describes relationships in the company; defines organizational roles, functions, capabilities, and limitations; and identifies the responsibilities for expeditionary signal companies during large-scale combat operations.

This publication includes 6 chapters and 1 appendix.

Chapter 1 discusses the operational environment and threats.

Chapter 2 provides an overview of the different roles, duties, and responsibilities within expeditionary signal companies, including the roles of units and the roles of key personnel within the companies.

Chapter 3 discusses the planning process from planning considerations to recovery operations.

- Section I is an overview of the operations process—planning, preparation, execution, and assessment.
- Section II discusses planning considerations.
- Section III discusses troop leading procedures at company level.
- Section IV discusses purposes, types, and methods of rehearsals and pre-combat checks and inspections.
- Section V discusses recovery.

Chapter 4 discusses support to operations.

- Section I discusses reception, staging, onward movement, and integration.
- Section II discusses command post support.
- Section III discusses organizations requiring tactical communications support for augmentation.
- Section IV discusses homeland defense and humanitarian support.
- Section V discusses support relationships.

Chapter 5 discusses sustainment operations.

- Section I discusses support to maintenance operations.
- Section II discusses signal supply management.

Chapter 6 discusses training in the company.

- Section I discusses collective training techniques, training environments, battle drills, combined arms training strategy and the eight step training model.
- Section II details how to apply signal assessment tables I–VII in the company.

Appendix A discusses recognizing and responding to electromagnetic warfare and cyber attacks.

This page intentionally left blank.

Chapter 1

Operational Environment and Threat

This chapter discusses the operational environment and threat. Section I outlines the contested and congested nature of the operational environment. Section II discusses the various types of state and non-state threat actors who pose risks to expeditionary signal companies.

UNDERSTANDING THE ENVIRONMENT

1-1. Factors that affect operations extend far beyond the boundaries of a commander's assigned area. An *operational environment* is the aggregate of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). An operational environment encompasses physical areas of air, land, maritime, space and cyberspace domains.

1-2. For the Army, the *cyberspace domain* is the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunication networks, computer systems, embedded processors and controllers, and relevant portions of the electromagnetic spectrum (FM 3-0).

1-3. Understanding the operational environment is essential for signal leaders, engineers, planners, system operators, and cybersecurity professionals to plan and execute effective signal support. *The Department of Defense information network* is the set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone (JP 6-0).

1-4. Various characteristics of an operational environment impact a unit's ability to operate and communicate. Leaders should consider the following aspects of the operational environment when planning and conducting operations:

- Congested and contested electromagnetic spectrum.
- Threats.
- Vulnerabilities.
- Risks.
- Hazards.

CONGESTED ELECTROMAGNETIC SPECTRUM

1-5. Expeditionary signal companies operate in a congested environment. The extensive use of the electromagnetic spectrum creates competition for bandwidth resources. All forces and supporting agencies depend on access to the electromagnetic spectrum for communications, information collection, and electromagnetic warfare (EW) capabilities. Signal systems rely on the electromagnetic spectrum for network transport. *Network transport* is the processes, equipment, and transmission media that provide connectivity and move data between networking devices and facilities (FM 6-02). For this reason, gaining and maintaining access to the electromagnetic spectrum is critical

for signal support to joint and Army operations. Refer to ATP 6-02.70 for more information about spectrum management operations.

CONTESTED ELECTROMAGNETIC SPECTRUM

1-6. Expeditionary signal companies also operate in a contested environment. The expeditionary signal battalion or corps signal brigade S-3 plans and delivers a robust communications network to mitigate the effects of a contested environment. Contested communications environments exist due to threat actions to degrade or deny access to the electromagnetic spectrum within the assigned area. See appendix A for more information on tactics, techniques, and procedures to recognize and respond to threat effects in a contested environment.

1-7. Expeditionary signal company elements should be familiar with and implement electromagnetic protection techniques to enhance survivability. *Electromagnetic protection* is the division of EW involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability (JP 3-85). Enemy attacks may combine electromagnetic attacks, other information warfare effects, or lethal fires to deny friendly forces the use of spectrum-dependent systems. To accomplish this goal, threat forces gather technical and combat information about friendly forces. As enemy forces locate and identify friendly units, enemy information warfare elements establish priorities to—

- Jam communications assets.
- Deceptively enter radio networks.
- Interfere with the normal flow of U.S. and allied communications.
- Target for lethal fires.

THREATS

1-8. A *threat* is any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland (ADP 3-0). Threats can be categorized as adversaries, enemies, or insider threats. An *adversary* is a party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged (JP 3-0). An *enemy* is a party identified as hostile against which the use of force is authorized (ADP 3-0). Insider threats present unique challenges because they are trusted individuals with access to Army capabilities and sensitive operational information. Threats may include individuals or groups, organized, or not organized.

1-9. Threats are a fundamental part of an overall operational environment. A threat can disrupt, destroy, or intercept the flow of information while operating from the other side of the world. Threats use an array of capabilities and methods to threaten Army systems and networks.

PEER THREAT

1-10. A peer threat is an adversary or enemy with capabilities and capacity to oppose United States forces across multiple domains worldwide or in a specific region where they enjoy a position of relative advantage. Unlike the previous two decades of counterinsurgency, peer threats will actively target and prioritize communications assets

on the battlefield during combat. Peer threats understand that without use of cyberspace and space domains, the Army loses its advantage during competition below the level of armed conflict, during crisis, and in armed conflict.

1-11. Peer threats can employ resources across multiple domains to create lethal and nonlethal effects throughout an operational environment (ADP 3-0). Peer threats generate tactical, operational, and theater strategic-level challenges that may be orders of magnitude more challenging than the previous two decades of counter insurgency operations.

1-12. Peer threats have the capability to degrade, disrupt, or destroy communication systems an expeditionary signal company employs through lethal fires, EW, and malicious cyberspace activities. An expeditionary signal company communications backbone supports the joint force's ability to carry out operations at echelons above brigade. Communications disruptions can severely hinder the commander's ability to employ the joint force.

Soldiers assigned to an expeditionary signal company need to understand what capabilities peer threats can employ to degrade or destroy their networks. Those capabilities are—

- Jamming and exploitation.
- Malicious cyberspace activities.
- Direct and indirect lethal fires.

HYBRID THREAT

1-13. Hybrid threat is the diverse and dynamic combination of regular forces, irregular forces, terrorists, or criminal elements unified to achieve mutually benefitting effects (ADP 3-0). Some aspects of the hybrid threat, such as criminal or terrorist organizations, do not abide by the law of armed conflict. Hybrid threats seek to exploit asymmetric advantages over an adversary to avoid engaging in direct combat.

1-14. The hybrid threat understands that the most challenging environment for the U.S. forces is one where conventional military operations occur in concert with irregular warfare. Enemies may employ malicious cyberspace activities and exploitation, battlefield jammers, and space-based capabilities, such as anti-satellite weapons, to disrupt U.S. communications; positioning, navigation, and timing; synchronization; and freedom of maneuver. The hybrid threat concept is not only making do with what is available, but deliberately taking advantage of all tools at hand to create a complex operational environment. Refer to FM 6-02 for more information about hybrid threat effects on signal support.

INSIDER THREAT

1-15. The considerations for insider threats are significantly different from those for individual hackers and small groups. Insider threats present a significant risk to military operations. An *insider threat* is a person with placement and access who intentionally causes loss or degradation of resources or capabilities or compromises the ability of an organization to accomplish its mission through espionage, providing support to international terrorism, or the unauthorized release or disclosure of information about the plans and intentions of U.S. military forces (AR 381-12). Insider threats are hostile

actors who intentionally compromise national security through deliberate actions. Insider threat should not be confused with operations security or cybersecurity risks, where sensitive operational information may be accidentally compromised and place U.S. operations or personnel at risk.

1-16. An insider threat is not always a military member or government employee. Third-party vendors, contractors, and partners could pose a threat as well. The insider threat is especially dangerous because insider activity is generally the hardest to identify. Downloading or printing files to remove from secure areas may appear to be ordinary day-to-day activities. Like enemy malicious cyberspace activities, a trusted insider can steal sensitive data to undermine partner relationships or manipulate public opinion. Refer to FM 6-02 for a more complete discussion of threats and the risks they present to signal support.

Chapter 2
Organization of Signal Support Elements

This chapter provides a brief overview of the expeditionary signal battalion, expeditionary signal battalion-enhanced, and their companies. It discusses their capabilities and the roles and responsibilities of key support staff and duty positions.

UNIT ORGANIZATION

2-1. The company's ability to accomplish its mission is dependent upon proper training to provide signal support, sound leadership, and the motivation of its signal teams. Company signal support must maintain operational focus. That is, the company must tailor signal plans to the supported commander's mission and intent.

2-2. Teams must be knowledgeable in their military occupational specialties and able to integrate their equipment into the Department of Defense information network-Army (DODIN-A). The *Department of Defense information network-Army* is an Army-operated enclave of the Department of Defense information network that encompasses all Army information capabilities that collect, process, store, display, disseminate, and protect information worldwide (ATP 6-02.71). An *enclave* is a set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter (CNSSI 4009).

EXPEDITIONARY SIGNAL BATTALION

2-3. Certain units do not have organic signal assets. However, they still need the same information technology services and applications as maneuver units when deployed. The pooled assets of an expeditionary signal battalion are available to provide them communications support.

2-4. The expeditionary signal battalion provides nodal and extension communications for deployed Army and joint units. Supported headquarters may include combatant commands, theater armies, joint task force headquarters, or joint force land component commands with no organic communications assets or units at echelons corps and below with insufficient assets for an assigned mission. The expeditionary signal battalions provide modular support. They employ small, medium, and large network teams as needed to meet specifically tailored support requirements. Refer to FM 6-02 for more information about requests for communications support. See figure 2-1 on page 6 for an expeditionary signal battalion organization chart.

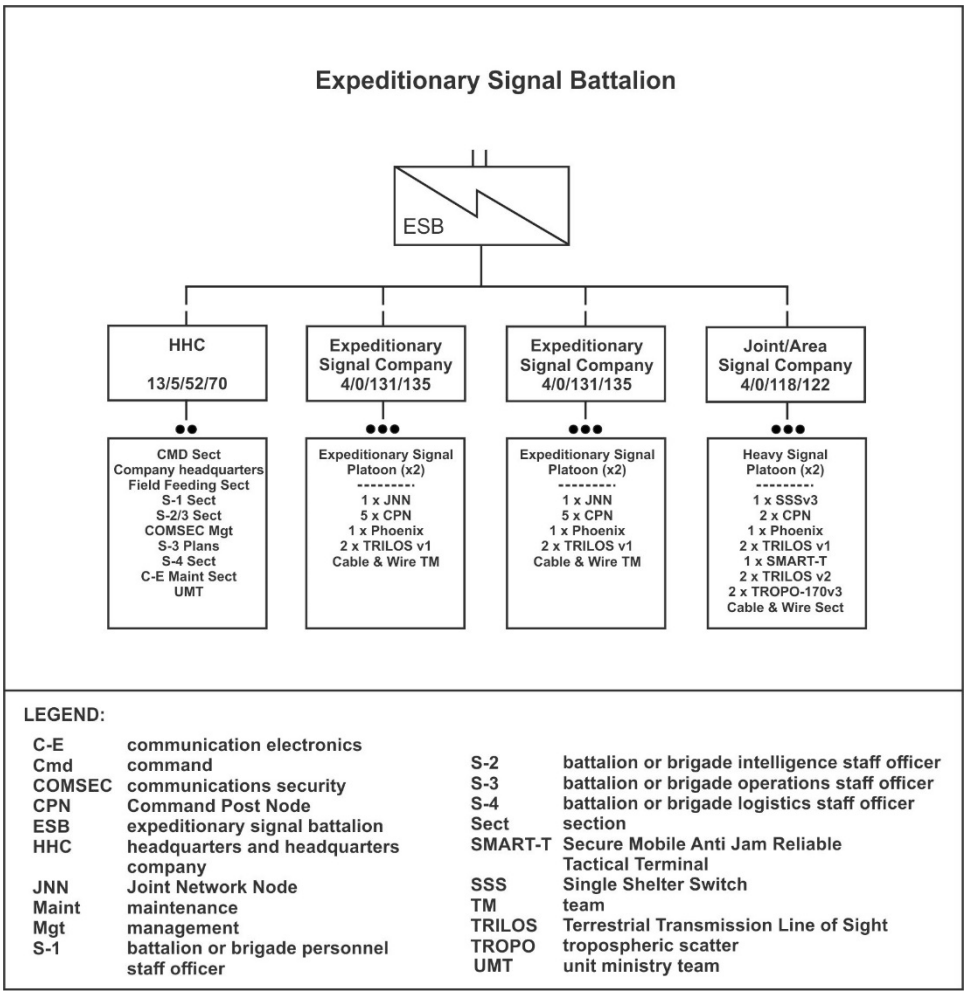


Figure 2-1. Expeditionary signal battalion organization chart

2-5. The expeditionary signal battalion's Tactical Network Transport at-the-halt systems provide network centric waveform satellite communications (SATCOM) to interface with the regional hub node and other network centric waveform equipped units.

2-6. The expeditionary signal battalion provides—

- Command and control for its assigned expeditionary signal companies and joint and area signal companies.
- Staff planning and network management for the battalion's communications assets.
- Communications-electronics maintenance support for network restoration.
- Continuous voice and data communications for supported units in austere environments.

2-7. Companies assigned to the expeditionary signal battalion are dependent upon the headquarters and headquarters company for logistical, personnel and administrative, religious, legal, and finance support. When required, companies receive support from—

- Joint command, theater army, corps, or division elements to provide field feeding and Army Health System support.
- Elements of the theater army or corps for supplemental transportation support.

EXPEDITIONARY SIGNAL COMPANY

2-8. The expeditionary signal company consists of a headquarters element and two expeditionary signal platoons. The battalion headquarters and headquarters company augment the company headquarters as necessary. See figure 2-2 on page 8 for the expeditionary signal company organization chart.

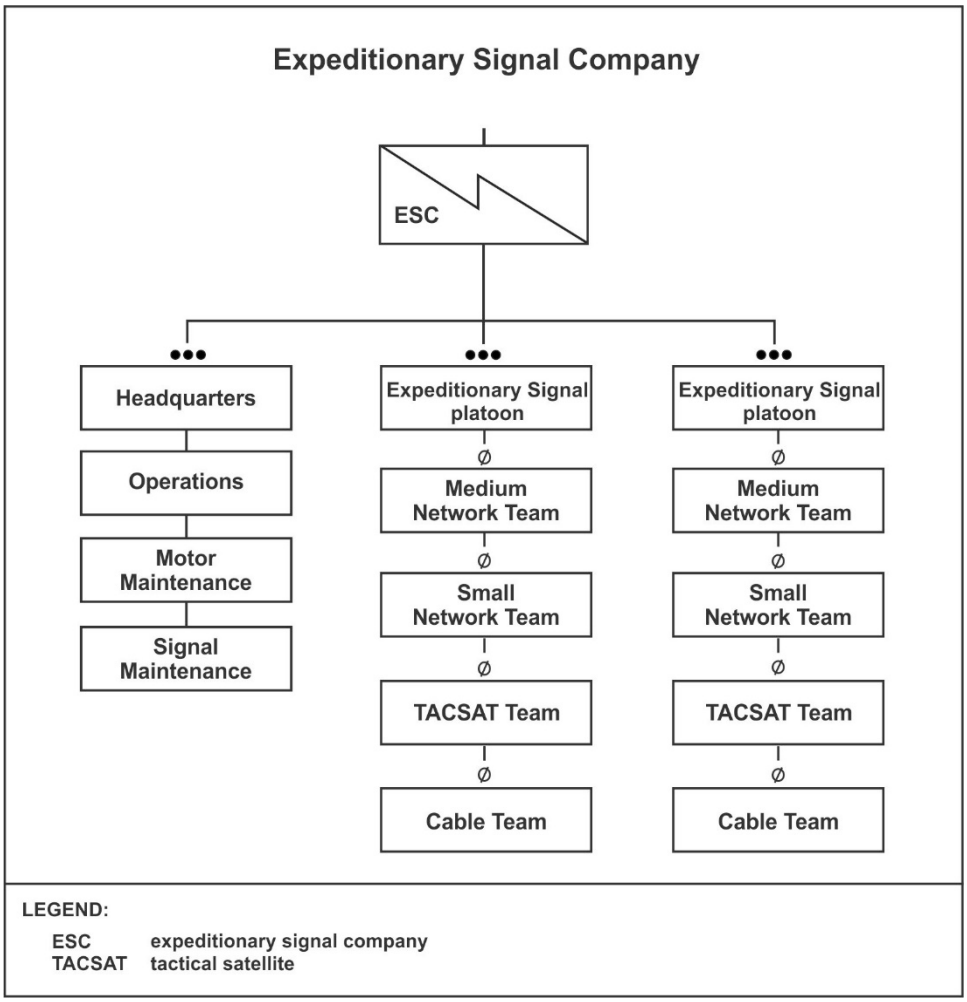


Figure 2-2. Expeditionary signal company organization chart

Capabilities

2-9. The company provides communications support for echelons above corps, major subordinate commands, theater army headquarters, or joint force headquarters.

2-10. The company provides Defense Information Systems Network and command and control-enabling services to small and medium command posts. This includes line of sight and beyond line of sight network transport, network management, and cable and wire systems. The expeditionary signal company provides tailored communications packages to support a particular mission.

Company Headquarters

2-11. The company headquarters provides limited administrative and logistical support for the company, which includes unit administration for assigned or attached elements;

supply support; chemical, biological, radioactive, and nuclear defense support; and weapons support. The company commander exercises command and control. The company operations section provides training, tactical planning, and support for unit operations.

2-12. The motor maintenance section provides field maintenance for automotive, power generation, environmental control equipment, and all classes of supply for the company and headquarters, headquarters company when co-located. Field maintenance is on-system maintenance, repair and return to the user including maintenance actions performed by operators. *Classes of supply* are the ten categories into which supplies are grouped to facilitate supply management and planning (JP 4-09). See chapter 5 for maintenance and classes of supply.

2-13. The signal maintenance section provides limited sustainment maintenance for organic communications-electronics, controlled cryptographic items, and communications security (COMSEC) equipment. *Communications security* is protective measures to deny unauthorized access to information of value derived from use of communications systems (JP 6-0).

2-14. When the company deploys as a complete communications support package, the company headquarters can conduct internal maintenance operations, with additional logistical support from higher as required. Commanders identify internal sustainment operations requirements during the operations process.

Expeditionary Signal Platoon

2-15. The expeditionary signal platoon installs, operates, and maintains one medium network node, five small network communications nodes, associated line of sight transmission systems and wideband satellite communications terminals, and performs network management. The platoon has an organic cable team that interconnects platoon assets and can support small to medium command posts. The platoon can dispatch individual teams to support separate missions or combine with other teams, platoons, or companies to meet mission requirements at any echelon.

Medium Network Team

2-16. A medium network team installs, operates, and maintains a Joint Network Node. The Joint Network Node allows tactical network connectivity for a medium command post supporting up to 200 end users. The medium network team provides a supported unit access to Defense Information Systems Network services necessary to conduct command post operations with reachback to the home station.

2-17. The Joint Network Node uses wideband SATCOM and line of sight systems as its means of network transport. Satellite transport is accomplished using its associated Satellite Transportable Terminal. The satellite transmission link between the Joint Network Node and the regional hub node is the frequency division multiple access backbone connection that provides connectivity to Defense Information Systems Network services.

2-18. The Satellite Transportable Terminal uses frequency division multiple access or time division multiple access to establish beyond line of sight connectivity between medium and small network teams.

2-19. A medium network team installs, operates, and maintains high-throughput line of sight transmission systems. The line of sight team provides high-throughput data transport connectivity between medium and small network teams. The use of line of sight systems establishes redundancy within the wide-area network and provides quality of service support throughout. The medium network team consists of nine personnel:

- 1x Senior network communications specialist.
- 1x Senior transmission system operator.
- 2x Network communications specialist.
- 2x Transmission system operator.
- 3x SATCOM systems operator-maintainer.

Small Network Team

2-20. The small network team installs, operates, and maintains a Command Post Node with its associated line of sight terminal. The small network team extends the tactical network established by the medium network team and provides access to Defense Information Systems Network services to small command posts with up to 20 users.

2-21. A small network team installs, operates, and maintains high-throughput line of sight transmission system and data transport connectivity between medium and small network teams. The use of line of sight systems establishes network transport redundancy within the wide-area network. Employing line of sight transport for short-range communications provides greater data throughput and reduces the need of satellite bandwidth while allowing dynamic routing.

2-22. The Command Post Node uses SATCOM or line of sight transport to the Joint Network Node. The Satellite Transportable Terminal provides alternate transport between the Command Post Node and its associated Joint Network Node using time division multiple access SATCOM. The Satellite Transportable Terminal operates over either military Ka or commercial Ku band. The small network team consists of six personnel:

- 1x Senior transmission systems operator.
- 2x Information technology specialist.
- 3x Transmission system operator.

Tactical Satellite Team

2-23. The tactical satellite (TACSAT) team installs, operates, and maintains the Phoenix terminal. The Phoenix terminal provides high capacity, inter- and intra-theater range extension to the DODIN-A. The Phoenix terminal provides SATCOM support to units or organizations that require the ability to transmit and receive large amounts of data.

2-24. The Phoenix terminal provides added bandwidth and reception capability compared to the Satellite Transportable Terminal. The Phoenix terminal operates in military X or Ka frequency bands or commercial C or Ku frequency bands using frequency division multiple access waveform only. X band transport allows the Phoenix

to transmit directly to a DOD gateway for connection to Defense Information Systems Network services without the use of a regional hub node. The Phoenix can transmit one satellite uplink while receiving up to four satellite downlinks simultaneously. The Phoenix can also transport logistical data to support such systems as the Global Combat Support System-Army. The TACSAT team consists of two SATCOM systems operator-maintainers.

Cable Team

2-25. The cable team provides fiber optic and coaxial cables to support Joint Network Nodes, Command Post Nodes, Satellite Transportable Terminals, and the Phoenix terminal. Personnel from the cable team deploy to locations to engineer aerial cable runs, buried cable runs, and cable runs through manholes. Cable teams build, install, and repair network cable runs in operations cells and command posts for Voice over Internet Protocol phones, computers, peripherals, and video teleconferencing. The cable team consists of three personnel:

- 1x Senior cable system installer.
- 2x Cable system installer.

JOINT AND AREA SIGNAL COMPANY

2-26. The joint and area signal company consists of a headquarters element and two heavy signal platoons plus any augmenting elements, personnel, or material assets. The battalion headquarters and headquarters company augment the joint and area signal company headquarters. See figure 2-3 on page 12 for the joint and area signal company organization chart.

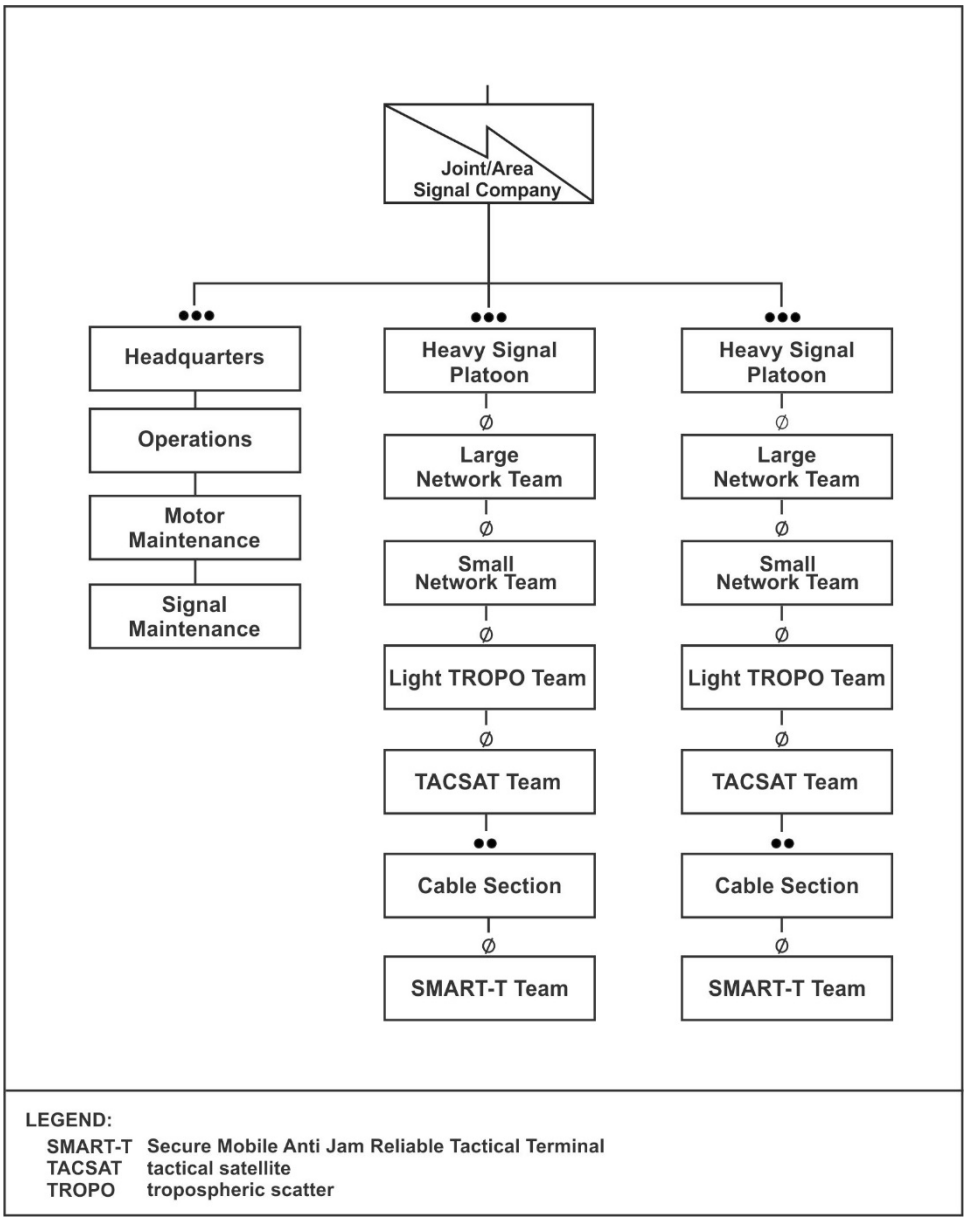


Figure 2-3. Joint and area signal company organizational chart

Capabilities

2-27. The joint and area signal company can extend communications systems support to a deployed force. The company is employed throughout a theater to provide communications support from brigade to theater army, joint task force, and combatant command.

2-28. The company provides access to Defense Information System Network and command and control-enabling services to large and medium command posts and command post clusters. This includes line of sight and beyond line of sight network transport, network management, and cable and wire systems. The joint and area signal company provides tailored communications packages consisting of one or more of the equipment systems shown in table 2-1 on page 14.

Table 2-1. Equipment allocations in the joint and area signal company

	Team type						
Equipment type	***TACSAT***	***Large network***	***Medium network***	***Small network***	***Light TROPO***	***SMART-T***	***LOS v3***
Phoenix	2	—	—	—	—	—	—
Single Shelter Switch	—	2	—	—	—	—	—
STT	—	2	—	4	—	—	—
SMART-T	—	—	—	—	—	2	—
TROPO	—	—	—	—	4	—	—
CPN	—	—	—	4	—	—	—
LAN manager	—	—	—	4	—	—	—
CCE	—	2	—	—	—	—	—
*HCLOS v1	—	—	—	4	—	—	—
**HCLOS v3	—	—	—	—	—	—	2

Legend:

CCE	Commercial Coalition Equipment
CPN	Command Post Node
HCLOS	High Capacity Line of Sight
LAN	local area network
LOS	line of sight
SMART-T	Secure Mobile Anti-Jam Reliable Tactical Terminal
STT	Satellite Transportable Terminal
TACSAT	tactical satellite
TOE	table of organization and equipment
TRILOS	Terrestrial Transmission Line of Sight
TROPO	tropospheric scatter

Notes:

* The HCLOS V(1) is modernized in the objective TOE to AN/TRC-238(V)2 (TRILOS V2). This is a one for one replacement.

** The HCLOS V(3) is modernized in the objective TOE to AN/TRC-238(V)1 (TRILOS V1). Due to the enhanced capability of the TRILOS, the quantity is reduced from 4 to 2, one per Joint Network Node.

Company Headquarters

2-29. The joint and area signal company headquarters provides limited administrative and logistical support for the company, which includes unit administration for assigned

or attached elements; supply support; chemical, biological, radioactive, and nuclear defense support; and weapons support. The company headquarters provides command and control and logistical support for assigned sections and teams. The primary difference between the joint area signal company headquarters and the expeditionary signal company headquarters is the organizational structure and equipment assigned to be supported.

Heavy Signal Platoon

2-30. The heavy signal platoon consists of one large network team, one line of sight V(3) team, two Command Post Node teams, two line of sight V(1) teams, two light tropospheric scatter (TROPO) terminal teams, one TACSAT team, a Secure Mobile Anti-jam Reliable Tactical Terminal (SMART-T) team, and a cable section with two cable teams. With its larger switch terminals and additional beyond line of sight transmission capabilities, the platoon is suited to support large command posts, command post clusters, or support bases. The platoon can support battalion- and brigade-level command posts and can dispatch individual teams to separate support missions or to augment other teams, platoons, or companies to meet specific mission requirements.

Large Network Team

2-31. The large network team is responsible for the installation, operation, and operator-level maintenance of the Single Shelter Switch. The Single Shelter Switch is co-located with the expeditionary signal battalion headquarters and headquarters company at a large command post of up to 500 end users, and functions as the primary communications node for the expeditionary signal battalion's portion of the tactical network. The corps signal brigade or theater signal brigade S-3 can use a Single Shelter Switch to establish a network operations and security center, as well as plan and engineer the local area network. A Single Shelter Switch deploys to establish a network communications node for a large command post or command post cluster.

2-32. A large network team is responsible for installing, operating, maintaining, and performing operator-level maintenance of a High Capacity Line of Sight (HCLOS) V(3) or Terrestrial Transmission Line of Sight (TRILOS) Radio. All HCLOS are replaced in the objective table of organization and equipment by the TRILOS. Units who have not been fielded TRILOS will continue operating the HCLOS until fielding is complete.

2-33. The TRILOS provides a substantial increase in bandwidth in comparison to the HCLOS radio system, with a significant reduction in size, weight, and power. TRILOS allows the ability to transport up to three line of sight transmissions from one antenna. The TRILOS (V)1 can transport up to six line of sight transmissions from two antennas attached to one antenna base. The TRILOS (V)2 can transport up to three line of sight transmissions from one antenna. The TRILOS can operate in a satellite denied environment. The TRILOS can transmit and receive three separate line of sight transmissions with one antenna mast. The TRILOS allows line of sight transmissions between communications nodes throughout the theater. The TRILOS small form factor provides a significant reduction in size, weight, and power compared to the HCLOS radio.

2-34. The HCLOS V(3) is the primary means of data transport between the Single Shelter Switch and its associated Command Post Nodes, using terrestrial microwave radio systems capable of up to 16 megabits per second of data throughput. The HCLOS V(3) allows greater bandwidth than the Satellite Transportable Terminal, but is limited to line of sight distance—approximately 40 kilometers (25 miles).

2-35. Command Post Nodes use HCLOS V(1)s to create a transport link with the HCLOS V(3) co-located with the Joint Network Node. A HCLOS V(3) may be used to establish a transport radio link to the HCLOS V(3) co-located with a Single Shelter Switch. The HCLOS V(3) can handle up to three separate line of sight transmissions multiplexed and forwarded to the Joint Network Node over one line of sight link. The large network team consists of six personnel:

- 1x Network communications system manager.
- 1x Senior network communications systems specialist.
- 4x Network communications system specialist.

Small Network Team

2-36. The small network team is responsible for the installation, operation, and operator-level maintenance of a Command Post Node, each accompanied with a Satellite Transportable Terminal V(2) as part of its inventory. A small network team has a HCLOS system. The Command Post Node extends the tactical network established by the Single Shelter Switch and provides access to Defense Information Systems Network services to small command posts with a maximum of 20 users. See paragraph 2-20 for more information about small network teams.

Light Tropospheric Scatter Team

2-37. The light TROPO team is responsible for the installation, operation, and operator-level maintenance of a TROPO transmission system. These systems provide beyond line of sight communications transport and reduce SATCOM demands by offering an alternative long-haul communications transmission method. TROPO transmission systems offer greater distance and bandwidth than the HCLOS systems and allow beyond line of sight communications transmission in a satellite denied environment. The light TROPO team consists of three personnel:

- 1x TROPO team supervisor.
- 2x TROPO systems operator.

Tactical Satellite Team

2-38. The TACSAT team is responsible for the installation, operation, and operator-level maintenance of the Phoenix terminal. See paragraph 2-23 for more information about TACSAT teams.

Secure Mobile Anti-Jam Reliable Tactical Terminal Team

2-39. The SMART-T team is responsible for the installation, operation, and operator-level maintenance of a SMART-T. The SMART-T is a protected satellite transmission system. It enables commanders at brigade and higher the ability to operate in an EW threat environment including radio frequency jamming, signal detection, and geographic

location threats. SMART-T can provide a protected link out of an EW threat environment, by landing an advanced extremely high frequency link at a Teleport and accessing the Defense Information Systems Network via Global Agile Integrated Transport where available. The SMART-T team consists of one network communications systems specialist.

Cable Team

2-40. The cable team is responsible for engineering fiber optic and coaxial cable runs for the Single Shelter Switch, Command Post Nodes, Satellite Transportable Terminals, and the Phoenix. See paragraph 2-25 for more information about the cable section.

EXPEDITIONARY SIGNAL BATTALION-ENHANCED

2-41. The expeditionary signal battalion-enhanced maintains the capability of the expeditionary signal battalion mission by providing tactical network connectivity to Defense Information Systems Network services specifically for theater armies, corps, and division-level units. Support for all other Army formations at echelon without organic signal support including joint, allied, coalition, and governmental organizations in expeditionary environments is available. The battalion is scalable to support small command posts at the maneuver company level up to large command posts at the theater level. See figure 2-4 on page 18 for the expeditionary signal battalion-enhanced organization chart.

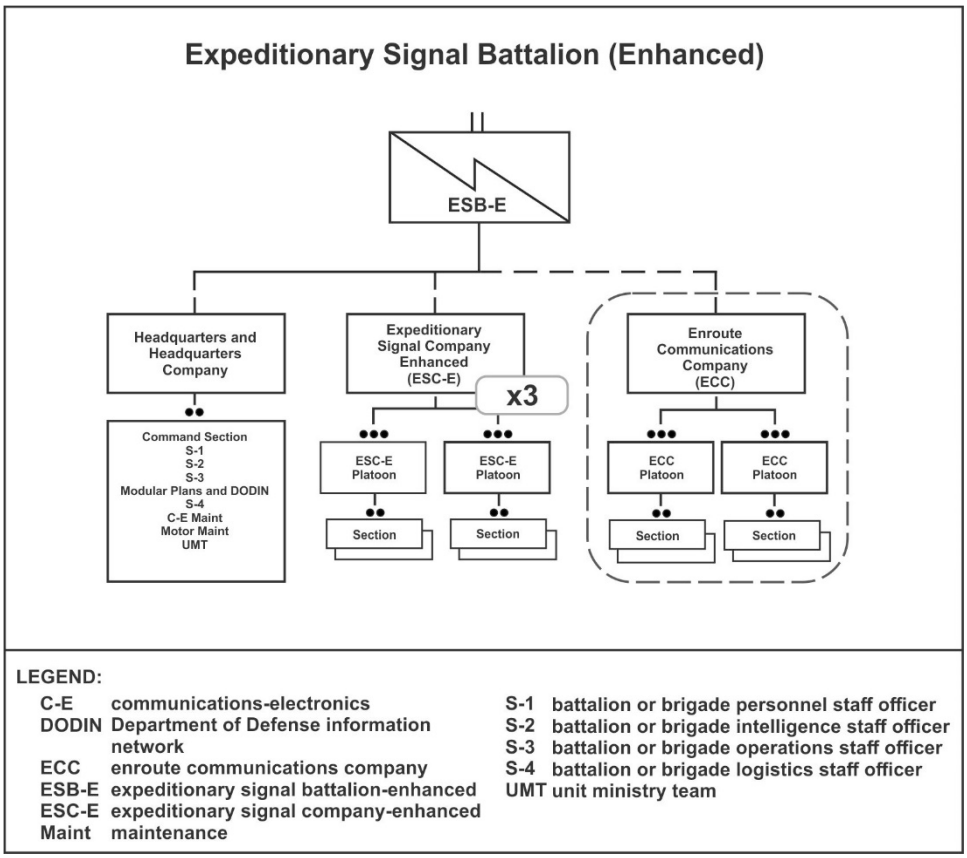


Figure 2-4. Expeditionary signal battalion-enhanced organization chart

2-42. An expeditionary signal battalion-enhanced can provide communications support for—

- Up to 12 small command posts that can support up to six users each that will offset the quantity of supportable medium command posts available. Communications support is provided using a small modular communications system (four total per company) and a sub-one-meter satellite antenna as satellite transport. Two personnel from one of the network support teams deploy with a small modular communications system. This configuration is typically for early entry operations. This reduces the number of supportable medium command posts.
- Up to 48 medium command posts that can support up to 48 users each. Communications support is provided using a medium modular communications system (16 total per company) and a 1.3-meter satellite antenna. One support team deploys in support of a medium command post. This configuration is considered the base support package for a battalion without organic signal support.
- Up to six large command posts that can support up to 350 users each that will offset the quantity of supportable medium command posts available.

Communications support provided by combining two medium modular communications systems and either a 2.4-meter satellite antenna, or Phoenix-E for satellite transport. A large command post configuration results from combining four of the network support teams and is considered a base support package for theater army.

2-43. The number of network support teams available for communications missions is contingent on the size of command posts that require communications support at a given time. Command post dispersion, threat-based survivability posture, and required capabilities vary by echelon and unit type, and contribute to unique support requirements. For example, if the battalion is supporting 48 medium command posts simultaneously, it cannot support additional small or large command posts. However, if the battalion provides support for two small command posts and one large command post simultaneously, it leaves only 42 network support teams for follow-on missions. Each command post variation has limitations related to bandwidth and throughput. Generally, the following variations align capability at echelon for units without organic signal support—

- Battalion without organic signal capabilities: 1 point of presence, 1 command post, 48 subscribers, and 1 medium command post.
- Brigade or group without organic signal capabilities: 2 points of presence, 2 command posts, 96 subscribers, and 2 medium command posts.
- Command or theater army without organic signal capabilities: 4 points of presence, 4 command posts, 192–350 subscribers, and 1 large command post.

2-44. Companies assigned to the expeditionary signal battalion-enhanced are dependent upon the headquarters and headquarters company for logistical, personnel and administrative support, religious, legal, and finance support. When required, companies receive support from—

- Elements within the theater for legal, Army Health System, finance, petroleum, oils, and lubricants and personnel and administrative service and support.
- Signal command (theater), corps signal brigade, or theater signal brigade for legal, Army Health System, finance, petroleum, oils, and lubricants, personnel, and administrative service and support.

EXPEDITIONARY SIGNAL COMPANY-ENHANCED

2-45. The expeditionary signal company-enhanced uses smaller, lighter equipment to enable more rapid deployment and maneuver across the battlefield. This means a smaller signal team is poised to go anywhere in the world and provide network services to supported users regardless of their mission set. This enables more flexible, robust, and resilient network connectivity.

2-46. The expeditionary signal company-enhanced consists of a headquarters element and two communications platoons. The battalion headquarters and headquarters company augment the company headquarters, as necessary. See figure 2-5 on page 20 for the expeditionary signal company-enhanced organization chart.

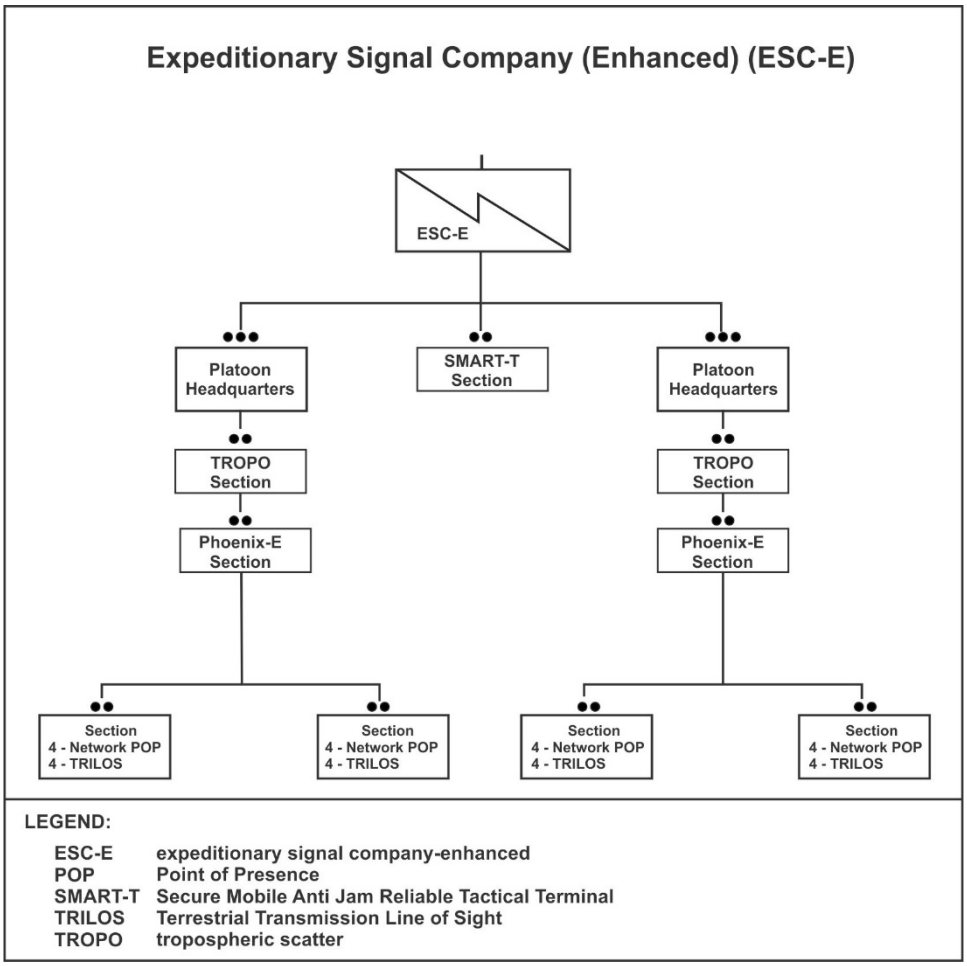


Figure 2-5. Expeditionary signal company-enhanced organization chart

2-47. The modular design of the expeditionary signal company-enhanced facilitates efficient allocation and task organization of the company's resources to meet a broad range of network support missions. Each network extension team is structured to provide a medium communications node. It can also downsize to create a small communications node or join other network extension teams to create a large communications node.

2-48. When required, modularized network equipment can move from one network extension team to another to tailor mission capabilities. This modular, scalable, and interchangeable design enhances the ability to task-organize teams with assets from within the company as needed to meet specific mission requirements.

Capabilities

2-49. The expeditionary signal company-enhanced equipment package includes a new medium ground satellite terminal and satellite antenna, known as the Scalable Network

Node. The Scalable Network Node can be established quicker than legacy systems to provide immediate network connectivity using its organic generators. This reduction in size enables the expeditionary signal company-enhanced to increase their network support capability to units with more nodes using less manpower and reduced transportation requirements. The SMART-T section belongs to the company and can be tasked as needed throughout the company depending on mission.

Company Headquarters

2-50. The company headquarters provides limited administrative and logistical support to the company, which includes unit administration for assigned or attached elements, supply support, and weapons support. The company performs limited field maintenance on organic communications-electronics and COMSEC equipment and all organic equipment for the company. The company headquarters provides command and control and logistical support for assigned sections and teams. See table 2-2 on page 22 for the expeditionary signal company-enhanced allocations.

Table 2-2. Equipment allocations in the expeditionary signal company-enhanced

	Team Type			
Equipment type	***SMART-T***	***TROPO***	***TACSAT***	***Network extension team***
TRILOS	—	—	—	4
VSAT	—	—	—	4
SNN	—	—	—	4
TROPO	—	2	—	—
SMART-T	1	—	—	—
CCE	—	—	—	4
Phoenix-E	—	—	2	—

LEGEND:

CCE	Commercial Coalition Equipment
Phoenix-E	Phoenix-enhanced
SMART-T	Secure, Mobile, Anti-Jam, Reliable Tactical Terminal
SNN	Scalable Network Node
TACSAT	tactical satellite
TRILOS	Terrestrial Transmission Line of Sight
TROPO	tropospheric scatter
VSAT	very small aperture terminal

Note. Company has a total of 14 CCE v4 and 2 CCE v2 distributed among the network extension teams.

Communications Platoon

2-51. A communications platoon consists of four sections: TROPO, Phoenix-E, Scalable Network Node, and TRILOS. The network extension platoon installs, operates, maintains, and secures modular communications systems to establish network communications nodes for small to large command posts, depending on personnel and equipment configuration.

Network Extension Team

2-52. Each network extension team can provide communications support ranging from a very small entry package to a medium command post. When combined, the network extension sections can support a large command post, such as a theater army headquarters or joint task force headquarters with up to 350 end users. Each team provides supported units with access to the tactical network using communications equipment with a full suite of services providing access to Defense Information Systems Network services and multinational communications interoperability.

2-53. Each network extension team has SATCOM systems that provide primary beyond line of sight transmission using Ku, Ka, or X band using frequency division multiple access, time division multiple access, or network centric waveform, depending on mission requirements. For large command posts, the expeditionary signal company-enhanced employs either a Phoenix-enhanced terminal or a transportable tactical command communications heavy to provide sufficient bandwidth for larger command post needs. Transportable tactical command communications heavy provides satellite transport with sufficient bandwidth to support a large command post in a small size, weight, and power package.

2-54. Each network extension team provides line of sight connectivity using a TRILOS. TRILOS provides up to three line of sight links from one antenna. The TRILOS (V)1 can transport up to six line of sight transmissions from two antennas attached to one antenna base. The TRILOS (V)2 can transport up to three line of sight transmissions from one antenna. The TRILOS can transmit and receive three separate lines of sight transmissions with one antenna mast, allows line of sight transmissions between communications nodes throughout the assigned area.

2-55. The TRILOS provides signal path diversity in congested and contested environments. Additionally, TRILOS provides network enclaves that enable connectivity to commercial and coalition networks. The network extension team consists of three personnel:

- 1x Senior network communications system specialist.
- 2x Network communications systems specialist.

Tropospheric Scatter Team

2-56. Light TROPO systems provide secondary beyond-line of sight transport, decreasing reliance on satellite usage while providing the ability to transmit in a satellite-denied environment. Light TROPO offers greater distance and bandwidth than line of sight systems. Light TROPO provides these capabilities in a smaller size, weight, and power package in comparison to traditional TROPO systems.

Tactical Satellite Team

2-57. The TACSAT team is responsible for the installation, operation, and operator-level maintenance of the Phoenix terminal. See paragraph 2-23 for more information about TACSAT teams.

Secure Mobile Anti-Jam Reliable Tactical Terminal Team

2-58. The SMART-T team is responsible for the installation, operation, and operator-level maintenance of a SMART-T. See paragraph 2-39 for more information about SMART-T teams.

ENROUTE COMMUNICATIONS COMPANY

2-59. The enroute communications company consists of a company headquarters, three enroute signal support platoons, and one command and staff palletized airborne node platoon. The enroute communications company provides global response force units with critical in-flight command and control, plane-to-plane, and plane-to-ground

network communications, and situational awareness on board while enroute to a mission objective.

> ***Note.*** The enroute communications company is a separate numbered company attached to an airborne ESB-E. It receives command and control, and logistical support from an expeditionary signal battalion-enhanced.

Capabilities

2-60. The enroute communications company supports up to 29 airborne communications packages. The enroute communications company provides the ability for division, brigade, or battalion staffs to conduct mission planning and disseminate orders to subordinate units while enroute to the deployed theater. See figure 2-6 on page 25 for the enroute communications company organization chart.

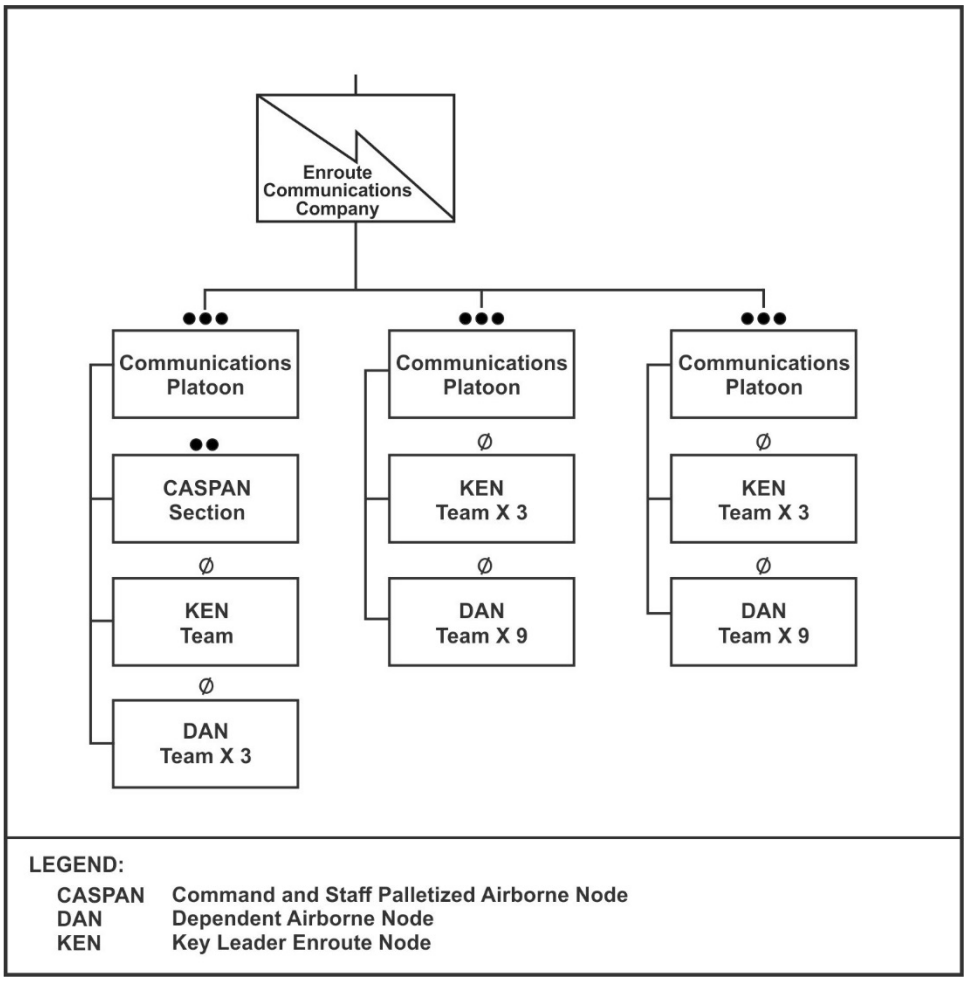


Figure 2-6. Enroute communications company organization chart

2-61. The enroute communications company provides in-flight connectivity to the tactical network, with the same secure voice, data, and video teleconferencing capabilities as ground command posts. The enroute communications company deploys the enroute command and control suite of systems using a fixed installed satellite antenna mounted on C-17 aircraft. The enroute command and control suite of systems includes—

- The Command and Staff Palletized Airborne Node.
- The Key Leader Enroute Node.
- The Dependent Airborne Node.

Table 2-3 on page 26 shows equipment allocations for the enroute communications company.

Table 2-3. Equipment allocations in the enroute communications company

Equipment Type	*Quantity*
Command and Staff Palletized Airborne Node	1
Key Leader Enroute Node	7
Dependent Airborne Node	21

Company Headquarters

2-62. The company headquarters provides personnel and facilities for command and control and administrative support of the company mission. The company commander and first sergeant—

- Direct company operations.
- Oversee company training, administration, and logistics functions.
- Supervise subordinate platoon leaders.

2-63. Support functions include supply and limited small arms maintenance. The company headquarters does not have food service, fuel handling, or health service support capabilities. Another unit must provide those support functions.

Communications Platoon 1

2-64. The communications platoon 1 consists of one Command and Staff Palletized Airborne Node section, one Key Leader Enroute Node team, and three Dependent Airborne Node teams. The Command and Staff Palletized Airborne Node is a more robust enroute command and control suite capable of providing a task force commander the ability to exercise command and control while maintaining situational awareness with continuous air-to-ground reachback to the home station.

Command and Staff Palletized Airborne Node

2-65. The Command and Staff Palletized Airborne Node can communicate air-to-air with both the Key Leader Enroute Node and Dependent Airborne Node systems. The Command and Staff Palletized Airborne Node provides the task force commander's staff the ability to conduct mission planning while enroute to a mission objective. The Command and Staff Palletized Airborne Node comes complete with seating and monitors for the task force commander. The Command and Staff Palletized Airborne Node team consists of three personnel:

- 1x SATCOM systems supervisor.
- 1x SATCOM systems specialist.
- 1x Network communications systems specialist.

Key Leader Enroute Node Team

2-66. An enroute signal support platoon consists of three Key Leader Enroute Node teams. The platoon provides air-to-air command and control and allows air-to-ground reachback to the home station while in flight to the operational area. A Key Leader Enroute Node can support up to three Dependent Airborne Nodes. The company deploys a Key Leader Enroute Node team to provide battalion commanders, executive officers,

and staff beyond line of sight, in-flight air-to-air command and control communications capabilities with subordinate company commanders and allows air-to-ground reachback to the home station for near real-time situational awareness while enroute to a mission objective. The Key Leader Enroute Node team consists of three personnel:

- 1x Senior network communications system specialist.
- 2x Network communications systems specialist.

Dependent Airborne Node Team

2-67. An enroute signal support platoon includes nine Dependent Airborne Node teams. The platoon provides air-to-air command and control and allows air-to-ground reachback to the home station while in flight to the operational area. The Dependent Airborne Node requires connectivity with a Key Leader Enroute Node for air-to-air and air-to-ground communications capability. The Dependent Airborne Node must be within 80 kilometers of a Key Leader Enroute Node.

2-68. Dependent Airborne Node teams install, operate, and maintain a dependent airborne node system that provides a company commander with the capability to maintain air-to-air communications with the battalion commander while on separate but adjacent flights. Each Dependent Airborne Node team provides communication link through narrowband (single-channel) TACSAT voice and line of sight voice and data capabilities to battalion and company commanders in-flight. The Dependent Airborne Node team consists of two network communications systems specialists.

Communications Platoon 2

2-69. The communications platoon 2 consists of three Key Leader Enroute Node teams and nine Dependent Airborne Node teams. The platoon provides air-to-air command and control and allows air-to-ground reachback to the home station while in flight to the operational area. The Dependent Airborne Node requires connectivity with a Key Leader Enroute Node for air-to-air and air-to-ground communications capability. The Dependent Airborne Node must be within 80 kilometers of a Key Leader Enroute Node. A Key Leader Enroute Node can support up to three Dependent Airborne Nodes.

ROLES AND RESPONSIBILITIES

2-70. Signal company Soldiers have primary roles and responsibilities; however, success depends on leaders working together. The company operates and maintains its assigned equipment and functions as one to fulfill its collective role.

2-71. The roles within an expeditionary signal company are—

- Company commander.
- First sergeant.
- Operations officer.
- Platoon leader.
- Platoon sergeant.
- Network communication system manager.
- SATCOM operations noncommissioned officer.
- Section sergeant.
- Team leader.

- Signal operators.

COMPANY COMMANDER

2-72. The company commander is ultimately accountable for the actions and performance of the company and is responsible for both its successes and failures. The company commander must know each platoon's capability and how to employ them and their equipment. The company commander must—

- **General—**
  - Be responsible for company discipline, training, maintenance of assigned equipment, and mission success.
- **Training—**
  - Direct unit collective training using the signal assessment tables.
  - Develop and submit the company training schedule for approval in accordance with the Army Training Plan.
  - Ensure operators and teams are proficient on their assigned systems.
- **Planning—**
  - Understand troop leading procedures and develop the ability to apply them quickly and efficiently.
  - Conduct troop leading procedures to plan company operations with the help of the first sergeant, operations sergeant, platoon leaders, platoon sergeants, and other key personnel.
  - Analyze the elements of the operational environment that support the higher commander's intent and concept of operations within the company's assigned mission.
  - Be a subject matter expert in the tactical employment of the company's capabilities.
  - Provide the commander's intent, within higher headquarters' intent, to the company.
- **Preparation—**
  - Know and understand the company's mission and the higher commander's intent.
  - Review company requirements based on the tactical plan.
  - Understand and frame risk decisions and mitigation strategies.
- **Execution—**
  - Execute missions in accordance with the higher commander's intent and vision, ensuring that all objectives are met, and goals are achieved.
  - Maintain situational understanding to ensure mission success.
  - Maintain network situational understanding and ensure seamless communication between units.
  - Analyze relevant friendly and enemy tactical updates and disseminate them to subordinates.
  - Maintain situational understanding of friendly position updates, overlay updates, and digital reports.
- **Sustainment—**
  - Request any support the company needs to perform its mission through the chain of command.
  - Develop and sustain situational understanding of network status and coordinate support with adjacent units and higher headquarters.

- **Maneuver—**
  - Synchronize with the supported command to ensure cyberspace and DODIN operations, within the scheme of maneuver, are agile and responsive to operational requirements.
  - Employ the company's capabilities to support the higher commander's intent and concept of operations.
  - Conduct maneuver operations to achieve the company's assigned mission, while minimizing risk and maximizing effectiveness.
  - Coordinate with adjacent units and higher headquarters to ensure a unified effort and achieve the desired end state.
  - Adapt to changing situations and adjust the company's maneuver plan accordingly.

FIRST SERGEANT

2-73. The first sergeant is the most senior enlisted member in the company and advises the company commander. The first sergeant is responsible for maintaining and enforcing the standards, developing the Soldiers in the unit, the administrative functions, and ensuring the health, welfare, and morale of the Soldiers and their Families. The first sergeant operates where the commander directs or where duties are required. The first sergeant must—

- **General—**
  - Execute and supervise routine operations such as SOPs; planning and coordinating training; personnel and administrative actions; and supervising supply and maintenance operations.
  - Assist and advise the company commander on all matters related to the company.
  - Manage talent within the company, ensuring proper delegation of work and optimal utilization of personnel.
  - Maintain responsibility for the medical and administrative readiness as well as the deployable status of the company.
  - Oversee the professional development and career management of subordinate noncommissioned officers.
- **Training—**
  - Provide oversight of the company training, ensuring alignment with the commander's intent and priorities.
  - Drive the implementation of the 8-step Training Model.
  - Monitor and evaluate individual and collective training based on the unit's approved mission essential task list.
  - Operationalize the commander's intent by developing and implementing training plans that focus on development of teams and individuals.
  - Prioritize training events and resources to ensure that the company is prepared to accomplish its mission.
- **Planning—**
  - Balance the commander's intent with mission requirements, ensuring the company is postured to success in a dynamic and changing environment.
  - Collaborate with the company commander and other key leaders to develop and refine operation orders.

- Assist the commander with analyzing operational gaps in the company and the plan.

- **Preparation—**
  - Mentor platoon leaders, platoon sergeants, and other noncommissioned officers on tactical and technical employment of the company's assigned equipment.
  - Ensure the company is prepared to operate in a variety of environments, including expeditionary and deployed settings.
- **Execution—**
  - Monitor and assess the company's performance during operations, providing feedback and guidance to subordinate leaders and individuals as needed.
- **Sustainment—**
  - Oversee the maintenance and repair of company's electronic equipment, ensuring it is completed in accordance with established procedures and standards.
  - Conduct daily sustainment, logistics, or administrative status reporting to higher headquarters.
- **Maneuver—**
  - Enable the commander's intent by applying troop leading procedures and the mission variables of mission, enemy, terrain and weather, troops and support available, time available, civil considerations, and informational considerations—METT-TC (I).
  - Ensure the company is postured to operate in a dynamic and changing environment, with a focus on expeditionary signal operations that are agile, responsive, and secure.

OPERATIONS OFFICER

2-74. The operations officer is the company primary sustainment planner and coordinator, reporting directly to the commander. During preparations for the operation, they work closely with the first sergeant to determine specific support requirements of the tactical plan. The operations officer will—

- **General—**
  - Manage company operations, maintenance, and property.
  - Oversee the company operational readiness and ensure compliance with unit standards.
  - Serve as the commander's principal advisor on operations and be prepared to assume command in the commander's absence.
- **Training—**
  - Oversee training development plans to enhance company capabilities and readiness.
  - Coordinate with the commander and first sergeant to identify training requirements and objectives.
- **Planning—**
  - Assist the commander in planning and coordinating signal operations, including network architecture, frequency management, and communications security.

- Develop and refine the signal operations plan and signal annex, ensuring alignment with the unit's operational plan.

- **Preparation—**
  - Coordinate with platoon leaders and platoon sergeants to ensure preparedness for deployment, including equipment readiness and personnel preparation.
  - Conduct rehearsals and inspections to ensure the company is prepared to execute its signal mission.
- **Execution—**
  - Monitor and report on signal operations, providing situational awareness to the commander and recommending adjustments to the signal plan as needed.
  - Coordinate with the signal platoons to ensure effective and efficient execution of the signal mission.
- **Sustainment—**
  - Compile logistics status updates from the platoon leaders, platoon sergeants, the first sergeant, and the company maintenance team and provide the updates to the commander.
  - Ensure the company executes supply and resupply operations in collaboration with the first sergeant.
  - Lead the company resupply rehearsal in cooperation with the first sergeant.
- **Maneuver—**
  - Coordinate with the commander and platoon leaders to plan and execute signal support in support of maneuver, including movement and re-deployment of signal equipment.
  - Ensure the company's signal assets are positioned to support the tactical plan, maintaining situational understanding and adapting to changing circumstances.

PLATOON LEADER

2-75. The platoon leader is accountable for the platoon's actions and performance and is responsible for overseeing all aspects of platoon operations, including tactical employment, training, administration, personnel management, and logistics. The platoon leader considers priorities of work and resupply to ensure the platoon is prepared for operations. The platoon leader consolidates logistics status reports for the platoon and keeps the commander informed of the platoon's operational status as situations change. Platoon leaders are responsible for materiel often valued at millions of dollars including vehicles, weapons systems, sensitive items, and radios.

2-76. The platoon leader must know each platoon member's capabilities, and how to employ the platoon and its equipment. The platoon leader's responsibilities include—

- **Planning—**
  - Being a subject matter expert in the tactical employment of the platoon's capabilities.
  - Being responsible to the commander for the platoon's discipline and training, equipment maintenance, and mission success.
  - Understanding troop leading procedures and developing the ability to apply them quickly and efficiently.

- Analyzing the elements of the operational environment that support the commander's intent and concept of operations within the platoon's assigned area.
- Planning operations with the help of the platoon sergeant and other key personnel.
- Orchestrating communication procedures and methods, including the radio nets on which the platoon operates, and positioning considerations.

- **Preparation—**
  - Knowing and understanding the mission and the commander's intent.
  - Developing sector sketches and site defense plans.
  - Reviewing platoon requirements based on the tactical plan.
  - Ensuring the platoon receives and rehearses isolated Soldier guidance.
- **Execution—**
  - Being responsible for the accomplishment of all missions within the commander's intent.
  - Exercising control of the platoon during operations.
  - Maintaining awareness of the situation and going where needed to supervise, issue orders, and accomplish the mission.
  - Analyzing tactical situations; disseminating and filtering information; and employing the platoon's full capabilities to accomplish the mission.
  - Analyzing relevant friendly and enemy tactical updates and disseminating them to subordinates.
  - Maintaining situational awareness of friendly position updates, overlay updates, and digital reports.
  - Being prepared to assume duties as company commander according to the succession of command.
- **Sustainment—**
  - Assisting the platoon sergeant in planning and coordinating sustainment for the platoon.
  - Requesting any support the platoon needs to perform its mission through the chain of command.
  - Receiving on-hand status reports from the platoon sergeant and team chiefs during planning.
  - Assisting platoon members as necessary.
  - Conducting combat and operational stress control.
- **Maneuver—**exercising control of the platoon's tactical execution through disciplined initiative.

PLATOON SERGEANT

2-77. The platoon sergeant is the most senior enlisted member in the platoon. In the absence of the platoon leader, the platoon sergeant performs all duties of the platoon leader. The platoon sergeant must—

- **General—**
  - Assist and advise the platoon leader.
  - Maintain responsibility for the professional development and career management of subordinate noncommissioned officers.
  - Maintain accountability to the platoon leader for the training, discipline, and welfare of platoon members.

- Assist other platoon members as necessary.

- **Planning—**
  - Assist the platoon leader in planning operations with the help of other key personnel.
  - Assist the platoon leader in analyzing the elements of the operational environment that support the commander's intent and concept of operations within the platoon's assigned area.
- **Preparation—**
  - Provide professional development and advice to team chiefs, other noncommissioned officers, and the platoon leader on tactical and technical employment of the platoon's assigned equipment.
  - Supervise individual and crew training.
  - Ensure the platoon maintains all assigned equipment.
  - Maintain responsibility for the medical and administrative readiness and the deployable status of platoon members.
  - Monitor the morale, discipline, and health of platoon members.
- **Execution—**
  - Update the platoon leader on appropriate reports and forward any reports needed by the company Headquarters.
  - Take charge of task-organized elements in the platoon during tactical operations, including quartering parties and support elements.
  - Monitor the common operational picture to maintain awareness of the platoon's position relative to friendly elements, electromagnetic emitters, and existing or emergent threats.
  - Direct the platoon's casualty evacuation plan.
  - Refine tactical placement of platoon personnel.
  - Perform actions in tactical situations which complement those of the platoon leader.
  - Be prepared to support control and sustainment of distributed operations when teams are under tactical control of other elements.
- **Sustainment—**
  - Supervise the platoon's administration, logistics, and maintenance.
  - Ensure support supplies are present.
  - Provide the platoon leader on-hand status reports during planning.
  - Collect, prepare, and forward logistic status updates and requests to the first sergeant.
  - Coordinate and supervise platoon resupply operations.
  - Maintain platoon strength information; consolidate and forward the platoon's casualty report; and receive and orient replacements.
  - Coordinate the platoon's sustainment requirements.
  - Handle the personnel needs of each platoon member.

2-78. Platoon sergeants supervise the platoon's administrative, supply, and maintenance actions. The platoon sergeant distributes supplies by coordinating and supervising platoon resupply operations. The platoon sergeant identifies resupply locations, the types and amounts of supplies needed, the time required to conduct resupply, and any necessary security considerations. Platoon sergeants collect, prepare, and forward logistics status updates and requests to the platoon leader or first sergeant as directed.

Refer to ATP 6-02.2 for detailed responsibilities of platoon leaders and platoon sergeants.

NETWORK COMMUNICATION SYSTEM MANAGER

2-79. The network communication system manager provides advanced technical assistance to teams to troubleshoot and resolve above-user-level problems at the company level. The network communication system manager is a senior noncommissioned officer in the headquarters platoon.

SATELLITE COMMUNICATIONS OPERATIONS NONCOMMISSIONED OFFICER

2-80. The SATCOM operations noncommissioned officer provides advanced technical assistance to teams to troubleshoot and resolve above-user-level problems at the company level. The SATCOM operations noncommissioned officer is in the headquarters platoon.

SECTION SERGEANT

2-81. The section sergeant assists the platoon sergeant and supervises two or more signal teams. In the absence of the platoon sergeant, the section sergeant must be ready to assume the duties of the platoon sergeant. The section sergeant must—

- Assist and advise the platoon sergeant and platoon leader.
- Mentor team leaders and team members in the technical skills to install, operate, and maintain their assigned equipment.
- Supervise team-level training in their sections.
- Maintain responsibility for the professional development and career management of subordinate noncommissioned officers.
- Supervise individual and crew training within their sections and advise the platoon sergeant and platoon leader of training shortfalls.
- Update the platoon sergeant on appropriate reports.
- Take charge of task organized elements in the section during tactical operations, including support elements.
- Monitor the morale, discipline, and health of section members.
- Ensure assigned teams maintain all equipment.
- Participate in supervision of company-directed platoon resupply operations.
- Assist the platoon sergeant in collecting and preparing logistic status updates.
- Maintain accountability to the platoon sergeant and platoon leader for the training, discipline, and welfare of section members.
- Perform actions in tactical situations which complement those of the platoon sergeant and platoon leader.
- Assist assigned teams and other platoon members as necessary.

TEAM LEADER

2-82. The team leader acts as a member of the team while supervising the individuals' contributions to the team's collective task accomplishment. As the direct supervisor, the team leader is in the best position to monitor and evaluate team members' individual strengths and weaknesses and can recommend training topics and events to the section

sergeant, platoon sergeant, and platoon leader. The team leader supervises cross training within the team, so the loss of an individual does not cause the team to fail in its mission. Team leaders—

- Maintain strong technical skills across all equipment assigned to the team.
- Mentor team members in the technical skills to install, operate, and maintain their assigned equipment.
- Supervise Soldier training.
- Maintain responsibility for the professional development of team members.
- Update the section sergeant or platoon sergeant on appropriate reports.
- Monitor the morale, discipline, and health of section members.
- Ensure team members maintain all equipment.
- Assist the platoon sergeant in collecting and preparing logistic status updates.
- Maintain accountability of equipment issued to the platoon.

SIGNAL OPERATORS

2-83. The team's tasks and missions require team members to integrate their efforts into accomplishing crew tasks which cannot be performed by an individual. Individual team members need to become experts at their individual military occupational specialty tasks and those crew and team tasks to which they contribute. Because signal teams are relatively small, team members need to be familiar with the individual tasks of other team members. See chapter 6 for unit and team training.

This page intentionally left blank.

Chapter 3
Planning in the Company

The planning process is often more important than the final plan itself, as it provides commanders with a greater understanding of the enemy, environment, assigned tasks, and greater flexible response options when the situation unexpectedly changes or when opportunities arise.

SECTION I – THE OPERATIONS PROCESS

3-1. The company follows the same sequence their battalion does when executing the operations process—planning, preparation, execution, and assessment.

PLANNING

3-2. *Planning* is the art and science of understanding a situation, envisioning a desired future, and laying out effective ways of bringing that future about (ADP 5-0). Commanders apply command and control to ensure signal operations support the concept of operations. The warning order (WARNORD) includes pertinent signal-specific information such as—

- Specific communications elements needed—
  - TACSAT.
  - Retransmission.
  - Line of sight.
- Networking systems.
- Types of COMSEC needed.

3-3. Planning is an ongoing process and continues as necessary during preparation and execution. Parallel planning occurs when the company commander and battalion commander plan for the same mission at about the same time. Battalions and above plan using the military decision-making process; companies and platoons plan using troop leading procedures (see paragraph 3-47). Figure 3-1 on page 38 shows the parallel sequences of the battalion's military decision-making process and the company and platoon's troop leading procedures.

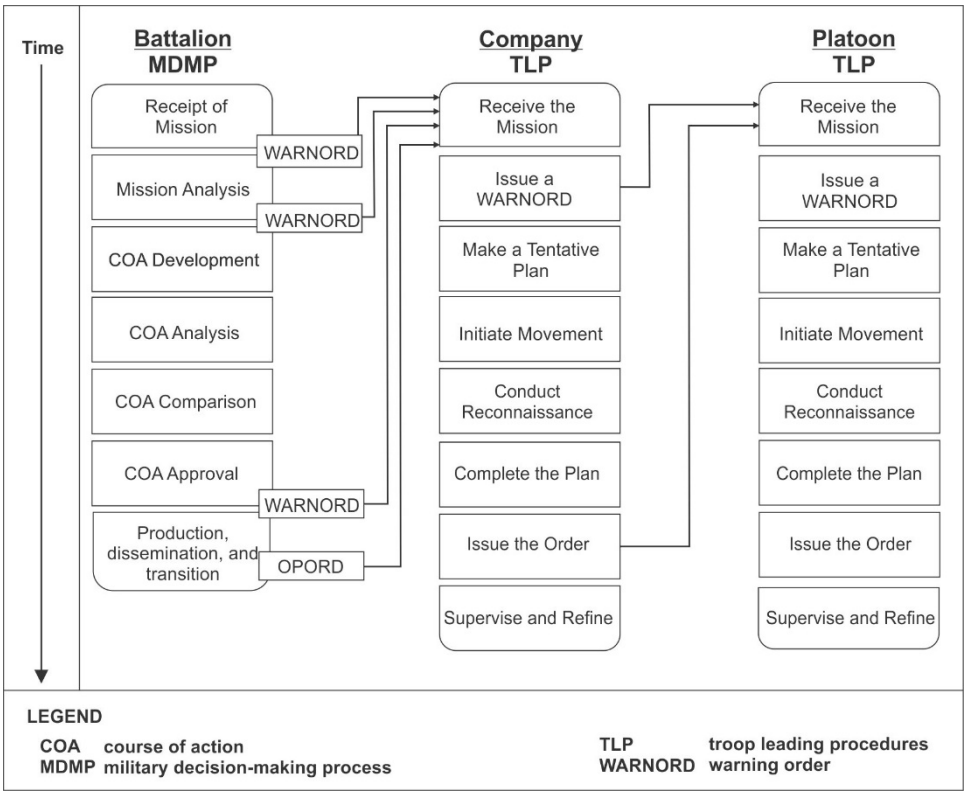


Figure 3-1. Parallel sequences of the military decision-making process and troop leading procedures

3-4. The company commander receives the mission and conducts troop leading procedures. After developing the plan, the company commander allows time for subordinate platoons to conduct rehearsals and supervises preparation prior to execution. The company then executes its mission while continuously assessing. Following execution, the company consolidates and reorganizes in preparation of a new mission starting a new cycle of the operations process.

PREPARATION

3-5. *Preparation* is those activities performed by units and Soldiers to improve their ability to execute an operation (ADP 5-0). Preparation activities include initiating information collection, preparing for DODIN operations, rehearsals, training, and inspections. Preparation requires the commander, staff, unit, and Soldiers' active engagement to ensure the force is ready to execute operations.

3-6. Preparation activities typically begin during planning and continue into execution. Preparation includes activities the company performs to improve its ability to execute its assigned tasks. Preparation includes—

- Plan refinement.
- Rehearsals (see section IV).

- Coordination.
- Checks and inspections.
- Movement.

3-7. During preparation, commanders need to create a timeline and analyze proposed signal sites—including terrain, weather, and enemy factors and how they affect the mission. Commanders capture all signal-specific guidance and identify facts, assumptions, and essential tasks from the operation order (OPORD).

3-8. Expeditionary signal company commanders should be in communication with the unit requesting the signal support to ensure all preparations are made prior to the start of the mission. Units that require signal augmentation do not request a unit, such as an expeditionary signal company, or a communications assemblage, but the operational capability required to accomplish their mission. The requesting unit G-6 or S-6 identifies the signal requirements. Accurately defining requirements simplifies the process of validation as the request routes through successive levels of the chain of command.

3-9. A detailed and customized standard operating procedure (SOP) standardizes common techniques and procedures to accomplish the company's missions to allow Soldiers to execute routine tasks with minimal supervision. When consistently executed and updated after each mission, the SOP can increase the commander's time available to plan and prepare for assigned tasks. The most effective SOPs are ones developed with input from all leaders in the company.

3-10. Commanders should maintain a running estimate that includes all signal information, including—

- Signal equipment on-hand.
- Signal equipment in-use.
- Non-mission-capable equipment.
- Equipment available to support the mission.
- The use of EW on the battlefield and its effects.

EXECUTION

3-11. Friction and uncertainty, especially enemy actions, dynamically affect plans. An accurate situational understanding that accounts for new realties that affect plans provides the basis for commanders to exploit opportunities or counter threats. Major activities of execution include—

- Decision making.
- Directing action.
- Assessment.

ASSESSMENT

3-12. Assessment refers to the continuous monitoring and evaluation of the current situation, particularly the enemy, along with the progress of the assigned task or tasks. Assessment entails—

- Continuously assessing the enemy's reactions and vulnerabilities, which may lead to windows of opportunity to exercise disciplined initiative.

- Continuously monitoring the situation and progress of the operation toward the company commander's desired end state.

3-13. Commanders should ensure their subordinates communicate effectively with their supporting DODIN operations section and that the unit SOP establishes reporting processes.

SECTION II – PLANNING CONSIDERATIONS

3-14. As battalion signal planners define communications requirements, one consideration should include the survivability of both personnel and equipment. *Survivability* is all aspects of protecting personnel, weapons, and supplies while simultaneously deceiving the enemy (JP 3-34). Examples of survivability include cover, concealment, and ensuring standoff between transmission equipment and operation areas. *Cover* is protection from the effects of fires (FM 3-96), whereas *concealment* is protection from observation or surveillance (FM 3-96).

DEPLOYMENT AND EMPLOYMENT OF UNITS

3-15. A robust network of satellites, radios, and other tactical communications systems enables units to connect to the DODIN-A regardless of their location. These unique capabilities enable the joint force commander to perform missions that are interdependent and globally dispersed.

PRE-DEPLOYMENT

3-16. Battalion signal planners prepare detailed signal plans, which include the satellite access request, frequency clearance, landing rights, deployment orders, deployment instructions, and equipment cut sheets. Planners obtain combatant command J-6 approval before the satellite access phase of any wideband SATCOM mission. Upon receiving the satellite access authorization, the communications planner—

- Obtains frequency clearance and landing rights by coordinating through their higher command.
- Prepares terminal deployment orders and cut sheets that reflect the approved equipment settings for wideband SATCOM terminal and gateway terminal operators involved in the mission.

3-17. The wideband satellite communications operations center (WSOC) updates the control communications subsystem identified in the satellite access authorization for positive control. The expeditionary signal company commander ensures terminals deploy with properly maintained equipment and qualified operators.

DEPLOYMENT

3-18. The SATCOM terminal operator deploys, installs, operates, and maintains the terminal equipment. The terminal operator reconfigures and adjusts operating parameters according to direction from the WSOC to support various tactical missions. The SATCOM terminal operator's responsibilities include—

- Configuring the terminal according to the equipment cut sheets and technical manuals.

- Establishing and maintaining contact with the WSOC using the terminal's orderwire or other dedicated means of communications before accessing the satellite.
- Establishing an alternate means of control communications to maintain positive control if the orderwire is not available.
- Establishing and maintaining user communications according to equipment cut sheets.
- Reporting equipment problems—communications outages, loss of positive control, or terminal outage problems—promptly.
- Submitting 8-hour status reports to the WSOC.
- Helping the WSOC report, analyze, and resolve persistent or recurring interference incidents.
- Preparing joint spectrum interference resolution reports according to CJCSM 3320.02 and applicable Service guidelines in the case of unidentified electromagnetic interference.
- Coordinating with the WSOC to resolve network communications disruptions, implement changes in service during a mission, and disseminate control directives or other communications between the WSOC and other network terminal operators.
- Displacing the terminal as required by the commander or the communications systems managing element, coordinating the move with the WSOC and communications systems planning element, and re-accessing the satellite, as necessary.

UNIQUE PLANNING REQUIREMENTS

3-19. Planning for most network assemblages can be conducted through the Systems Planning, Engineering, and Evaluation Device (SPEED) software. However, leaders should not limit themselves to SPEED. SPEED is a modular software application that provides capabilities to support communications planning, spectrum management, radio frequency engineering and EW planning and analysis. SPEED is a government off-the-shelf program that is free to the DOD and federal agencies, and available through foreign military sales.

3-20. Network planners use SPEED to establish links compatible with the terrain and frequencies being considered. SPEED can be used for—

- Point-to-point network connections.
- Radio coverage analysis.
- High frequency communications.
- Asset management.

3-21. Outside of network planning, leaders ensure proper guidance and mission planning takes place. These considerations focus on the type of mission, duration, and support. Some of these considerations are—

- Communications planning meetings for this operation.
- The mission.
- The deployment timeline.
- Mission starting and ending dates.
- Supporting headquarters, and what information they require.

- Higher-level DODIN operations authority.
  - Expeditionary signal battalion.
  - Corps signal brigade.
  - Theater signal brigade.
  - Regional cyber center.
- Higher-level authority when augmenting—
  - Brigade combat team.
  - Division.
  - Corps.
  - Joint task force.
  - Signal command (theater).
  - Theater army.
  - Combatant command.
- Host-nation agreements and landing rights if the operation is outside the continental United States.
- Communications infrastructure in the assigned area.
- Whether existing communications infrastructure can be leveraged.
- Threat environment.
- Where required frequencies are obtained.
- Whether satellite-based positioning, navigation, and timing system frequencies are incorporated in the unit frequency plans to avoid interference from tactical communications equipment.
- Planning for the mission partner network.
- Planning for interoperability with multinational partners or other Services.
- Priorities for individual links.
- Terminals required to support the mission.
- Whether terminals are on hand or will be obtained from another unit.
- Where terminals will be located.
- What equipment and which troops will deploy.
- Redundant communications necessary.
- Whether there is a heavy dependence on one means of communication during the operation.
- Whether networks can combine, or time-share based on usage patterns.
- Whether teams have the needed personnel to move and operate all equipment.
- Whether redundant power supplies are operational and if so, for how long.

SATELLITE COMMUNICATIONS

3-22. SATCOM planners must predict that threats will contest the use of communications satellites. SATCOM resources are critical targets for threat antiaccess, and area denial capabilities. Due to heavy U.S. reliance on advanced SATCOM systems, such an attack may be a central focus of a threat antiaccess and area denial strategy, requiring a higher degree of situational awareness and planning for mitigation techniques.

3-23. Techniques to consider include—

- Formulating SATCOM plans that minimize the radio frequency footprint.

- Using modulation techniques which provide a low probability of signal detection or interception.
- Identifying bandwidth requirements (lower data rates require less radio frequency power).

3-24. SATCOM terminal operators must also be proactive and take appropriate actions to minimize the impacts of interference and threat attacks. Terminal operators should assess threat risks and the capabilities and vulnerabilities of terminals to plan and implement appropriate primary, alternate, contingency, and emergency (PACE) communication plans to assure communications and the ability to restore lost communications in operationally relevant timeframes. They must deploy with all necessary capabilities to enable the concept of support and the PACE plan. SATCOM users protect information sent over SATCOM; routinely check terminal performance; report degradation to operations centers identified in their satellite access authorizations; and be prepared to change terminal settings to mitigate interference and attacks when directed by an operations center.

3-25. Factors to consider include—

- PACE plans to mitigate threat effects in a congested or contested environment.
- Locating SATCOM antennas away from command posts to mitigate collateral damage if communications systems are destroyed.

Satellite Access Requests

3-26. When a unit has a validated requirement for SATCOM access, the brigade or battalion S-3 communications planner submits a satellite access request through higher headquarters to the theater army for validation. Once the combatant command validates the requirement, the regional satellite communications support center (RSSC) responsible for managing the SATCOM resources processes it. If sufficient satellite resources are available, the RSSC prepares a satellite access authorization after reviewing the validated request. If resources are not available, a satellite access request is denied or partially denied. If denied, the combatant command may request arbitration. Approved satellite access authorizations permit operational access. The RSSC issues them to the originating unit and the controlling WSOC on a secure website.

3-27. Planners should provide flexibility in the satellite access request by including all frequency bands their terminals can use. Doing so reduces the chance of denials or partial denials and increases the effectiveness of restoral by enabling planners to plan multiple communication paths for multi-band terminals. Often, power restrictions or capacity limitations in one band do not carry over to other bands, so the user can achieve better throughput and support if they are flexible and transparent.

3-28. Each satellite access request must meet CJCSI 6250.01 requirements. Failing to meet the requirements results in denial of satellite access. Units generate satellite access requests using automated (preferred) or manual systems. Planners should submit requests as early as possible. Additional time may be necessary to coordinate frequency conflicts within the organization. Procedures may vary depending upon the type of SATCOM support required-narrowband, wideband, protected, or commercial. When submitting a satellite access request, the requesting unit should follow the steps below:

- Signal or operations staff planners prepare a satellite access request.

- Unit forwards satellite access request to supported theater army SATCOM manager for validation; units in the continental United States submit requests to FORSCOM.
- The theater army or FORSCOM submits a request to the combatant commander for mission approval.
- The combatant commander forwards validated satellite access requests and gateway access requests to the supporting RSSC.

3-29. In accordance with CJCSI 6250.01, the validation authority (combatant command, FORSCOM) submits satellite access requests to the supporting RSSC at least 30 days before the requested access date. Validation authorities may require validation authorities or authorized users to submit a satellite access request and gateway access request well in advance of the 30-day minimum to meet applicable timeline requirements. Therefore, the combatant commands and FORSCOM require users to submit their request at least 51 days before the requested access date. The validation authority requires an exception to policy to justify the late submission signed by the first O-6 in the chain of command for requests not submitted 51 days in advance. If the requesting unit fails to submit a request at least 30 days before mission access or the RSSC determines a pattern of late requests, the RSSC may request an O-6 level engagement with the validation authority, along with a letter of lateness submitted by an O-6 sponsoring the requesting unit.

3-30. Satellite access requests for critical operations, such as Defense Support of Civil Authorities can be expedited based on priority. Unit training requests can also have different priorities. General unit training would have a lower priority than pre deployment training. Refer to CJCSI 6250.01 for submission, waiver, appeal requests, and precedence.

Gateway Access Requests

3-31. Planners submit a gateway access request to request Defense Information Systems Network services. The Defense Information Systems Agency reviews and approves gateway access requests. The gateway access request submission starts with the unit and routes through the chain of command to the theater army. If approved, the gateway access request routes through the respective RSSC and Defense Information Systems Agency offices. If approved, the RSSC sends the request to the Defense Information Systems Agency, and the authorization is assigned a satellite communications database number and priority.

Access Priorities

3-32. The Chairman of the Joint Chiefs of Staff sets priorities for military SATCOM systems. The Joint Staff J-6 collects, consolidates, assesses, and records requests and coordinates with the Joint Staff J-3 to validate and prioritize them.

3-33. The Chairman of the Joint Chiefs of Staff owns SATCOM assets and apportions them to each combatant commander, who temporarily controls the assets within their area of responsibility. Combatant commanders apportion resources to joint task forces or Service components, depending on operational requirements and national priorities.

3-34. SATCOM planners should have an endorsed satellite communications database requirement before submitting a satellite access request. Before submission to the RSSC, the expeditionary signal battalion communications planner prioritizes satellite access requests based on mission priorities according to the priority tables in CJCSI 6250.01. Some satellite communication planning considerations are—

- The types of terrain present that may interfere with SATCOM access or terminal placement.
- Whether SATCOM requirements are justified to support the mission.
- Whether requests for satellite communications database numbers are needed.
- Whether expedited SATCOM approvals are needed.
- How long SATCOM services will be required.
- Whether SMART-T will be needed, given the threat environment.
- Satellite access requests required—
  - Frequency division multiple access—Phoenix; Joint Network Node.
  - Time division multiple access—Joint Network Node; Command Post Node; Phoenix; Transportable Tactical Command Communications.
- Where required frequencies are obtained.
- The type of traffic that requires protected SATCOM links and the traffic that can use commercial SATCOM.
- The phasing of the operation and the type of SATCOM support necessary for each phase.
- Whether SATCOM operator-maintainers are qualified and available.
- Training required before movement.
- Whether SATCOM units and personnel are prioritized and included in the time-phased force and deployment data.
- Whether clear policies for the use of personal Global Positioning System receivers, handheld commercial radios, cell phones, and morale calls using SATCOM are established and disseminated.
- Whether SATCOM requirements for the operation have been evaluated to ensure the proper use of limited assets.
- Whether plans and provisions should be established for a changeover between TACSAT and commercial SATCOM.

Positive Control

3-35. Positive control is the continuous ability to oversee SATCOM access and coordinate necessary changes in the frequency or channel, power level, or network settings. Coordination of access can use alternative communication means (for example, radio, telephone, or orderwire) to help in the adjustment of power levels, frequency, and user modem settings with the regional satellite communications support center (RSSC) or WSOC guidance. All SATCOM access must be under positive control. If positive control is lost, the WSOC may terminate terminal access after coordination with the wideband consolidated satellite communications system expert. As the technology built into systems allow, positive control through automated methods will be used (CJCSI 6250.01). Wideband SATCOM terminals may access a satellite only under the conditions of positive control.

3-36. The WSOC—

- Monitors signals transmitted by a wideband SATCOM terminal over a given satellite.
- Communicates with the terminal operators to establish network communications matching the satellite access authorization.
- Maintains orderly network operation.

3-37. Monitoring includes verifying terminal type, location, transmit and receive frequency, data rate, coding, and spectral shape of each carrier. The WSOC may terminate network terminal access if the terminal causes unauthorized access or jamming. If changes in connectivity are necessary during a mission, the WSOC coordinates the change with the appropriate organizations.

LINE OF SIGHT COMMUNICATIONS

3-38. Line of sight terminals provide primary network transport between the large and small nodes throughout the wide-area network. Line of sight systems provide much greater bandwidth and lower operating costs than SATCOM and can transmit in satellite denied environments but need an unobstructed path to other line of sight systems.

3-39. Line of sight planning considerations include—

- Whether the selected site is free of obstructions.
- Whether line of sight communication is possible between nodes given terrain and data rate.
- Direction of line of sight path—preferably parallel to the forward line of own troops.
- Whether nodes are within 40 kilometers (25 miles) of each other.
- Whether frequencies are available.
- Whether threat EW is expected in the area.
- Whether the Network Module Software Planner is being used to create heat maps for each antenna.
- Whether the TRILOS needs to be used with HCLOS on multiple teams.

TROPOSPHERIC SCATTER

3-40. The operational environment and unit placement and types will determine where the TROPO transmission capability is required. TROPO transmission is planned either as the primary terrestrial transport capability or as an enhancement for terrestrial layer connectivity within the network. Planning and engineering for the TROPO transmission nodes will be provided by the parent network operations and security center. Some planning considerations are—

- Whether the command post is operating in disadvantaged terrain that does not allow line of sight.
- Whether the Unified Network Operations Planner software is the most recent version.
- Whether TROPO transmission is the primary or alternate terrestrial transport means.

SUPPORTED UNITS

3-41. Supported units have specific requirements regarding network access. Leaders should use the supporting unit's signal support request to establish baseline hardware and personnel requirements for the mission. Some unit planning considerations are—

- Who the supported unit is.
- What services are needed—
  - SECRET Internet Protocol Router Network.
  - Nonclassified Internet Protocol Router Network.
  - Joint Worldwide Intelligence Communications System.
  - Video teleconferencing.
  - Mission partner network.
  - Voice over Internet Protocol.
  - Voice over Secure Internet Protocol.
- Whether connectivity to cloud services is needed.
- Whether the supported unit has updated their command and control information systems.

Note. Supported units must provide their own end user equipment. Signal companies only provide network connectivity. Signal companies do not provide supported units with telephones or computer workstations.

COMMUNICATIONS SECURITY

3-42. Network planners develop a cryptonet plan to support the unit's operation plan or order. The planner bases the cryptonet plan on the communications plan. Network managers consider—

- The mission objective.
- Units that will participate in the mission.
- Communications required for the mission.
- Duration of the mission.
- Whether there are adequate COMSEC devices and keying material to support the network.
- COMSEC distribution plan.
- The plan for the emergency destruction of COMSEC and classified material in the terminals.
- Whether there are enough couriers to support the teams needed.
- How COMSEC will be provided to teams where direct transport is not possible—
  - Over the air distribution.
  - Through SECRET Internet Protocol Router Network.
  - Courier.

3-43. The network planner develops a cryptonet overlay and identifies COMSEC requirements for the mission based on the OPORD and communications plan. The Automated Communications Engineering Software workstation provides the ability to tailor the software to meet a variety of planning requirements. The Automated Communications Engineering Software includes a planning module for each network

category. The categories of network plans supported by Automated Communications Engineering Software include—

- Tactical networks.
- Combat net radios.
- General-purpose networks.
- Adaptive networking wideband waveform.

3-44. Battalion and below COMSEC responsibilities are limited to distributing signal operating instruction data and distributing loadsets and network timing. The company receives signal operating instructions, frequency hopping, and COMSEC data from the S-3. Expeditionary signal companies follow unit SOP when distributing COMSEC down to the team level.

COMMUNICATIONS PLATOON (ENROUTE COMMUNICATIONS COMPANY)

3-45. Enroute signal support platoon-specific planning considerations include—

- User requirements, such as how many users and what equipment needs to be supported. User requirements should be stated clearly in the signal support request, including which Internet Protocol addresses need to be advertised ahead of time.
- Whether the Air Force can support the signal support request, usually determined days prior to the mission start time which can and often does change on the flight line prior to boarding.
- Whether return flights for operators and equipment have been coordinated with the Air Force or commercial airlines.
- Whether the team leader has—
  - Return flight information and timelines from the Air Force or commercial airlines.
  - A point of contact for the supported unit.

JOINT FORCIBLE ENTRY PLATOON

3-46. The joint forcible entry platoon is an airborne platoon that supports early entry operations. Planning coordination must be made between the Air Force and supporting unit, including—

- User requirements such as how many users and what equipment needs to be supported. User requirements should be stated clearly in the signal support request including which Internet Protocol addresses need to be advertised ahead of time.
- Whether the Air Force can support the signal support request, usually determined days prior to the mission start time which can and often will change on the flight line prior to boarding.

SECTION III – TROOP LEADING PROCEDURES

3-47. Troop leading procedures provide commanders a framework for planning and preparing for missions. Smaller units—company and below—lack formal staffs and use troop leading procedures to plan and prepare for operations.

3-48. Commanders use troop leading procedures to solve tactical problems and use the first sergeant, platoon leaders, and platoon sergeants to help with the process. The type, amount, and timeliness of information passed from higher to lower directly affects the commander's troop leading procedures. Troop leading procedures consist of eight steps:

- Receive the mission.
- Issue a WARNORD.
- Make a tentative plan.
- Initiate movement.
- Conduct reconnaissance.
- Complete the plan.
- Issue the order.
- Supervise and refine.

3-49. Troop leading procedures provide a framework for planning and preparing for a company mission. Troop leading procedures begin when the commander receives the first indication of an upcoming mission and continue throughout the operations process. As each subsequent order arrives, commanders modify their assessments, update tentative plans, and continue to supervise and assess preparation.

3-50. The first three steps of troop leading procedures—receive the mission, issue a WARNORD, and make a tentative plan—normally occur in order. However, the sequence of subsequent steps takes place based on the situation. Initiate movement and conduct reconnaissance may occur several times. The last step—supervise and refine—occurs throughout the mission.

STEP 1 – RECEIVE THE MISSION

3-51. The commander receives the company's mission through a written or verbal WARNORD, OPORD, or FRAGORD from the battalion. Upon receipt of the mission, the commander conducts an initial assessment to determine the time available to accomplish the mission. The commander performs a cursory analysis of assigned tasks using the mission variables of mission, enemy, terrain and weather, troops and support available, time available, civil considerations, and informational considerations—METT-TC (I). A more advanced analysis of the mission variables occurs during step 2.

3-52. During this step, commanders also—

- Determine the time available to plan, prepare, and execute the mission.
- Determine the one-third-two-thirds timeline for leader planning and subordinate preparation (see paragraph 3-59).
- Prepare an initial planning timeline.

STEP 2 – ISSUE A WARNING ORDER

3-53. The company WARNORD is a preliminary notice to the company of an order or action to follow. Less detailed than a complete OPORD, a WARNORD aids in parallel planning. After commanders receive a new or updated mission and assess the time available to plan, prepare, and execute the mission, they immediately issue a company WARNORD.

3-54. In the initial company WARNORD, the commander includes the same elements given in the battalion commander's initial WARNORD, but company focused. If

practical, commanders brief subordinate leaders face-to-face using a rough terrain model, sketch, or map. Figure 3-2 shows an example of a WARNORD format.

[CLASSIFICATION]
(Change from verbal orders, if any) (Optional)

Copy ## of ## copies
Issuing headquarters
Place of issue
Date-time group of signature

WARNING ORDER [number] Example: WARNING ORDER #3

(U) References: *Refer to higher headquarters' operation plan (OPLAN) or operation order (OPORD) and identify map sheets for operation (Optional).*

(U) Time Zone Used Throughout the OPLAN or OPORD: *(Optional).*

(U) Task Organization: *(Provide initial task organization to include attachments and detachments.)*

1. (U) Situation. *The situation paragraph describes the conditions and circumstances of the operational environment that impact operations in the following subparagraphs:*

a. (U) Area of Interest.
b. (U) Area of Operations.
c. (U) Enemy Forces.
d. (U) Friendly Forces.
e. (U) Interagency, Intergovernmental, and Nongovernmental Organizations.
f. (U) Civil Considerations.

2. (U) Mission. *State the issuing headquarters' mission.*

3. (U) Execution.

a. (U) Initial Commander's Intent. *Provide brief commander's intent statement.*
b. (U) Concept of Operations. *This may be "to be determined" for an initial warning order (WARNORD).*
c. (U) Tasks to Subordinate Units. *Include any known tasks at time of issuance of WARNORD.*
d. (U) Coordinating Instructions.

4. (U) Sustainment. *Include any known logistic, personnel, finance, or health service support preparation tasks.*

5. (U) Command and Signal. *Include any changes to the existing order or state "No change."*

ACKNOWLEDGE:

[Commander's last name]
[Commander's rank]

OFFICIAL:

[Authenticator's name]
[Authenticator's position]

ANNEXES: *List annexes by letter and title.*

DISTRIBUTION: *List recipients.*

[page number]
[CLASSIFICATION]

Figure 3-2. Example warning order format

3-55. A WARNORD follows the five-paragraph OPORD format. Normally an initial WARNORD issued at echelons battalion and below includes—

- The mission or nature of the operation.

- The time and place for issuing the OPORD.
- Units or elements participating in the operation.
- Specific tasks not addressed by unit SOPs.
- The timeline for the operation.

3-56. An essential element of the WARNORD is the initial planning timeline, including instructions or information that will help subordinates prepare for the upcoming mission. Issuing the initial WARNORD as quickly as possible enables subordinates to maximize their planning and preparation time (parallel planning) while the company commander begins to develop the OPORD. Upon receipt of more information, the company commander issues an updated WARNORD, so subordinates have all relevant information available.

STEP 3 – MAKE A TENTATIVE PLAN

3-57. Commanders begin to develop a tentative plan after issuing the company WARNORD. They should not wait for a complete battalion OPORD before starting to develop a tentative plan.

MISSION ANALYSIS

3-58. The commander begins mission analysis immediately upon receipt of the mission from the battalion commander. During mission analysis, the company commander restates the given mission and conducts an initial risk assessment. Mission analysis helps the commander determine—

- The current situation.
- The company's mission.
- How best to accomplish the mission.
- The possible risks.

3-59. Though mission analysis is an ongoing process, the company commander adheres to the one-third, two-thirds technique to give subordinates sufficient time to prepare. One-third of the time available remains set aside for the commander to prepare and issue an order, while the remaining two-thirds of the time is for platoon leaders to disseminate the order to their platoons and prepare for the mission.

3-60. The commander will conduct a more in-depth mission analysis by evaluating the mission variables of METT-TC (I). The commander will brief the mission analysis results and their importance, enabling the company to recognize and seize opportunities during the mission.

MISSION VARIABLES

3-61. Mission variables describe characteristics of the assigned area and their impacts on a mission. The mission variables are—

- Mission.
- Enemy.
- Terrain and weather.
- Troops and support available.
- Time available.
- Civil considerations.

- Informational considerations.

3-62. During execution, continuous analysis of the mission variables enables the issuance of well-developed FRAGORDs. Commanders assess whether any new information presented during planning changes their mission and decide how to adjust the plan to meet these new conditions.

3-63. METT-TC (I) analysis does not need to occur in any order. How and when commanders analyze the variables depends on when they receive information and, on their experience, and preferences. One technique is to conduct parallel troop leading procedures based on the products received from the battalion.

Analysis of Mission

3-64. Commanders must understand the mission, intent, and operational concept one and two levels higher. Doing so makes it possible to exercise disciplined initiative and act to exploit limited windows of opportunity.

3-65. Commanders use the following to gain this understanding:

- Supported unit's mission, intent, and concept.
- Unit's purpose.
- Constraints.
- Specified, implied, and essential tasks.
- Restated mission.

3-66. Commanders ensure the unit provides critical communication to the supported units while also addressing logistical needs such as maintenance, housing, food supply, and mobility. Duties involve understanding—

- What services and capabilities the signal company delivers.
  - NIPRNET.
  - SIPRNET.
  - VTC.
  - Secure and nonsecure voice services.
- What supported unit will provide.
  - Billeting.
  - Logistics—supply and maintenance support.
  - Transportation.
  - Feeding.
  - Personnel and finance support.
  - Medical support.
  - Religious support.
- How expeditionary signal teams align with the theater network.
  - Gateway access.
  - DODIN operations technical channels.
  - Cyber incident reporting.
  - Joint spectrum interference resolution report.

Mission, Intent, and Concept (Two Levels Up)

3-67. Regardless of echelon, leaders must understand the concept of operations two levels up, identifying the tasks and purpose and how their immediate higher headquarters contributes to the operation. At company-level, this is the brigade commander's mission, intent, and concept. This information is found in paragraph three of the battalion OPORD, or in paragraphs two and three in the brigade OPORD.

Mission, Intent, and Concept (One Level Up)

3-68. Leaders must understand their immediate headquarters' concept of operations to identify their headquarters' task and purpose and their own contributions to the mission. At company-level, this is the supported unit commander's mission, intent, and concept. This information is found in paragraphs two and three of the battalion OPORD. Leaders also identify the tasks, purposes, and dispositions for supported command post elements and all adjacent signal elements under the supported unit's control.

Company's Purpose

3-69. The commander locates the company's purpose in the concept of operations in paragraph three of the battalion OPORD. The company's purpose helps achieve the purpose of the immediate higher headquarters. If company commanders are unclear of their purpose, they should ask the supported unit's commander for further explanation.

3-70. Understanding the supported unit commander's intent and purpose helps the company commander exercise disciplined initiative under the mission command approach. In the presence of new information, the commander knows the intent and purpose of the next higher headquarters and can adjust as needed to meet them. If all else fails, the company commander must be able to determine what the company must accomplish and why.

Tasks

3-71. Commanders must identify and understand the task or tasks required to accomplish a given mission. The three types of tasks are—

- *Specified task*—a task specifically assigned to a unit by its higher headquarters (FM 5-0). Specified tasks are found in paragraph three of the battalion OPORD, under tasks to subordinate units.
- *Implied task*—a task that must be performed to accomplish a specified task or mission but is not stated in the higher headquarters' order (FM 5-0). Implied tasks come from a detailed analysis of the battalion OPORD, enemy situation and course of action, terrain, and from knowledge of doctrine and history. Commanders rely on their experience and the experience of subordinate leaders to help identify the implied tasks.
- *Essential task*—a specified or implied task that must be executed to accomplish the mission (FM 5-0). Commanders either decide which tasks are essential or are told directly by the battalion commander. The essential tasks and the company's purpose are in the battalion OPORD paragraph three concept of operations if an implied task, or tasks to subordinate units if a specified task.

3-72. Some specified, implied, and essential tasks that directly affect the company may be written into an annex and not be included in paragraph three of the battalion OPORD. The commander should review, at a minimum, Annex C (Operations) from the supported unit's OPORD, if available and if time permits.

Constraints

3-73. A *constraint* is a restriction placed on the command by a higher command. A constraint dictates an action or inaction, thus restricting the freedom of action of a subordinate commander (FM 5-0). Constraints primarily appear in paragraph three of the supported unit's OPORD.

3-74. Examples of constraints for an expeditionary signal company may be resource limitations, such as class III or class V transport capacity, or in the operational environment, such as—

- Terrain or manmade structures that interfere with line of sight capabilities.
- Limited spectrum resources.
- The joint restricted frequency list.

Restated Mission

3-75. The commander concludes the mission analysis by restating the company mission. To do this, they determine the five Ws:

- Who—the teams required for the mission.
- What—the services the teams will provide.
- When—the time given in the OPORD.
  - Movement time
  - Time required on station.
  - Mission start date-time group.
  - Mission end date-time group.
- Where—the operations will occur (assigned area, objective, grid coordinates).
- Why—the signal team's purpose, taken from the supported unit's concept of operations.

Visual Aids

3-76. Commanders prepare or receive a graphic depiction of terrain to help explain their findings regarding the effects of terrain and weather on the mission. The graphic depiction of terrain can be a photograph, digital map, a map overlay, or a terrain model. In the graphic depiction, leaders show terrain mobility classifications, key terrain, intervisibility lines, known obstacles, avenues of approach, mobility corridors, and limitations of communications systems. Refer to ATP 2-01.3 for more information about visual aids.

Analysis of Enemy

3-77. The second mission variable to consider is the enemy. The S-2 provides an analysis of the enemy with which the company anticipates contact. Commanders need to know and understand the enemy's disposition, composition, strengths, doctrine (if known), equipment capabilities, vulnerabilities, and probable courses of action.

Additionally, the line between enemy combatants and civilian noncombatants is sometimes unclear and therefore requires the leader to understand the law of armed conflict, the rules of engagement, and the local situation.

3-78. Analyzing the enemy helps commanders understand what the enemy is doing and why. The commander determines—

- The capabilities of enemy weapons and other systems that may affect signal support—
  - Electromagnetic jamming.
  - Positioning, navigation, and timing jamming.
  - Manned and unmanned aircraft.
  - Intelligence, surveillance, and reconnaissance.
  - Long-range precision fires.
  - Irregular forces.
  - Malicious cyberspace activities.
- The enemy's most probable and most dangerous courses of action for signal units operating in the rear area:
  - Most probable—malicious cyberspace activities and electromagnetic jamming.
  - Most dangerous—long-range precision fires.

Assumptions

3-79. Commanders continually improve their situational understanding of the enemy and update their analog and digital enemy templates as new information becomes available. Commanders should bring deviations or significant conclusions reached during enemy analysis that could positively or negatively affect the supported unit's plan to the supported commander for awareness and, if necessary, action.

How the Enemy Will Fight

3-80. The commander should understand when, where, and how the enemy has historically used their assets. A threat template is a visual illustration of how the enemy force looks and acts without the effects of weather and terrain. The threat template should appear in the company OPORD or be made available from the S-2. This type of understanding is the starting point for the commander's enemy analysis.

3-81. Commanders must understand not only the enemy's capabilities but also how they will fight and the direct impact this has on signal support. Enemy EW effects can include—

- Disruption of tactical radios, satellite links, and data transmissions.
- Signal degradation.
- Loss of satellite-based positioning, navigation, and timing.
- Geolocating signal sites and targeting for lethal fires.

3-82. Enemy cyber effects can critically impair the signal company's mission and larger operational goals. Enemy malicious cyberspace activity effects can include—

- Breach of secure communications.
- Denial of Service attacks.
- System lockdown through malware in the network.

- Disinformation in the network.
- Data exfiltration.
- Modifying stored data on network.

3-83. The enemy may not fight using any form of structured or published doctrine. In such a situation, commanders rely on assessments made by the S-2.

Composition

3-84. Commanders determine the types of vehicles, soldiers, and equipment the enemy could use against the supported teams, including malicious cyberspace activities, electromagnetic attack and direction-finding capabilities.

Disposition

3-85. From the S-2's input, commanders determine how the enemy may be, arrayed, the echelon from where the enemy originated, and the disposition of the next two higher enemy elements. Previous terrain analysis also helps identify where the enemy may or may not be able to go, based upon the number and types of vehicles in their formation.

Strength

3-86. The commander may determine the strength of the enemy element templated in the company's assigned area by way of requests for information through the S-2.

Capabilities

3-87. The commander must know what weapon systems the templated enemy has. Knowing the maximum effective ranges of the enemy weapons systems, the commander can better determine the vulnerability of signal sites to lethal fires. Knowing the characteristics and capabilities of enemy cyberspace and EW capabilities, the commander can better recognize and respond to an enemy cyberspace or electromagnetic attack. Commanders should be familiar with the characteristics of the enemy units and enemy weapons platforms, including—

- Lethal fires capabilities.
- Cyberspace capabilities.
- EW capabilities.
- Manned and unmanned aircraft systems.
- Maneuver forces.

Recent Enemy Activities

3-88. Commanders can request any recent enemy activities in the assigned area from the S-2. Knowing what the enemy has done in the past may indicate likely future enemy courses of action.

Enemy Situation Template

3-89. The situation template is a refined version of the threat template, accounting for the effects of terrain, weather, and all previous enemy analysis. The commander should provide a detailed situation template to platoon leaders, either as an analog map overlay

or digital graphic. The situation template is portrayed one echelon lower than the one developed by the next higher headquarters. Additionally, leaders should incorporate the electromagnetic order of battle into the situation template to assist in identifying enemy electromagnetic spectrum-dependent capabilities and vulnerabilities. Refer to ATP 2-01.3 for situation template items.

INFORMATION REQUIREMENTS

3-90. A *commander's critical information requirement* is specific information identified by the commander as being essential to facilitate timely decision making. (JP 3-0) Commander's critical information requirements are based on the likely need for the commander to make specific decisions during the operation. A commander's critical information requirement is—

- Specified by the commander for a specific operation.
- Applicable only to the commander who specifies it.
- Situation dependent and directly linked to a current or future mission.
- Time-sensitive.

3-91. Commander's critical information requirements should change with the situation over time. Commanders will add and delete commander's critical information requirements as the situation changes. Commander's critical information requirements (see figure 3-3 on page 58) consist of priority intelligence requirements and friendly force information requirements:

- *Priority intelligence requirement*—the intelligence component of commander's critical information requirements used to focus the employment of limited intelligence assets and resources against competing demands for intelligence support (JP 2-0). Priority intelligence requirements are clear, answerable, focused on a single question, and necessary to drive an operational decision.
- *Friendly force information requirement*—information the commander and staff need to understand the status of friendly force and supporting capabilities (JP 3-0).

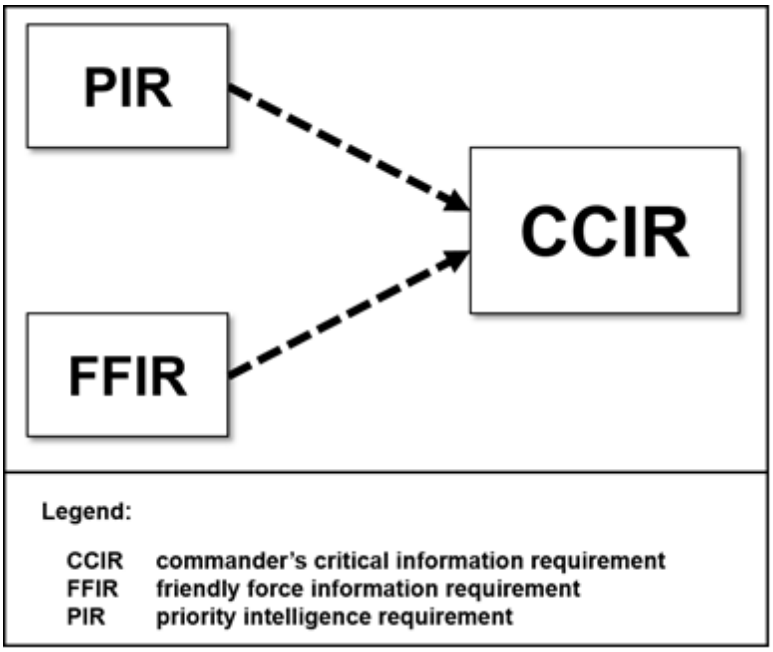


Figure 3-3. Commander's critical information requirements

3-92. The company may be directly or indirectly tasked to answer one or more of the commander's information requirements. The commander must ensure all personnel in the company know what to look for and to report changes to the status of friendly capabilities.

3-93. Essential elements of friendly information are not commander's critical information requirements, but are critical aspects of a friendly operation that, if known by the enemy, would compromise or lead to failure of the operation. Consequently, this information must be protected from identification by the enemy. Examples of essential elements of friendly information include the location of a command post or the signal operating instructions.

Analysis of Terrain and Weather

3-94. Analysis of terrain explains the terrain's effect on the mission. Commanders consider the effects of manmade and natural terrain in conjunction with the weather on friendly and enemy operations.

3-95. Terrain can be categorized as—

- **Unrestricted**—terrain free of restrictions to movement; no actions are needed to enhance mobility. For the signal company, unrestricted terrain typically is flat or moderately sloped, with scattered or widely spaced obstacles such as trees or rocks and no major terrain features or manmade structures that would interfere with—
  - line of sight signal propagation.
  - satellite look angles.

- **Restricted**—terrain hindering movement somewhat. Little effort is needed to enhance mobility, but units might have to adjust speed and formations, or make frequent detours. For the signal company, restricted terrain typically means moderate to steep slopes or moderate to dense spacing of obstacles such as trees, rocks, or urban structures. Mountains, steep hills, and manmade structures are examples of restricted terrain for signal forces.
- **Severely restricted**—terrain which severely hinders or slows movement of combat formations unless some effort is made to enhance mobility. Engineer forces might be needed to improve mobility, or the company might have to deviate from doctrinal tactics. Dense buildings and other structures, heavy vegetation, and valleys that interfere with communications links characterize severely restricted terrain for signal forces.

3-96. Terrain analysis should produce several specific conclusions for the commander:

- Templated locations of enemy forces, essential weapon systems, and lethal fires.
- Optimum positions for own assets.
- Thorough understanding of time and space relationships of events, leading to thorough contingency plans.
- Possible enemy indirect firing points.

3-97. Terrain analysis also identifies factors specific to signal support, including—

- Identification of areas which may increase the range of communications systems.
- Identification of areas where terrain interferes with line of sight capabilities and requires SATCOM for beyond line of sight communication.
- The company's ability to use natural or manmade features to mask the unit's electromagnetic signature.
- The company's ability to mask the unit's electromagnetic signature within the spectral noise of an urban area.

3-98. From the modified combined obstacle overlay developed by the S-2, commanders gain understanding of the general nature of the ground and effects of weather. They must go beyond passing along the modified combined obstacle overlay to their subordinates or making general observations of the terrain such as identifying high ground or streams. Commanders must conduct their own analysis and determine how the terrain and weather uniquely affect both the enemy and the company.

3-99. Following terrain analysis, commanders develop a graphic terrain analysis overlay. This product is similar to the modified combined obstacle overlay in that it shows the critical military aspects of terrain. The terrain analysis overlay facilitates planning and aids in briefing subordinates.

3-100. In general, terrain and weather do not favor one side over the other unless one is better prepared to operate in the environment or is more familiar with it. The terrain may, however, allow terrain masking to prevent enemy forces from detecting friendly electromagnetic signatures.

3-101. Commanders analyze terrain using the mnemonic of observation and fields of fire, avenues of approach, key terrain, obstacles and movement, and cover and

concealment to determine the effects of each aspect of terrain on friendly and enemy forces.

Obstacles

3-102. Commanders identify existing and reinforcing obstacles that might limit mobility or signal support in the assigned area:

- Existing obstacles—
  - **Natural**—includes rivers, forests, mountains, ravines, gaps, and ditches more than three meters wide, tree stumps and large rocks more than 18 inches high, forests with trees eight inches or more in diameter with less than four meters between trees.
  - **Manmade**—includes urban areas, canals, railroad embankments, buildings, power lines, or communications infrastructure.
- Reinforcing obstacles—
  - **Tactical**—inhibit the ability of the enemy to move, mass, and reinforce. Examples include mine fields (conventional and situational), anti-tank ditches, or wire obstacles.
  - **Protective**—offer close-in protection and are important to survivability.

3-103. Defensive considerations when analyzing obstacles and restricted terrain include—

- Where the enemy wants to go.
- What existing obstacles and restricted terrain may affect the enemy.
- How to protect signal systems from enemy detection using terrain masking techniques.

Avenues of Approach

3-104. An *avenue of approach* is a path used by an attacking force leading to its objective or to key terrain. Avenues of approach exist in all domains (ADP 3-90). Avenues of approach are classified by type (mounted, dismounted, air, or subterranean), formation, and speed of the largest unit traveling on it. An expeditionary signal company commander primarily focuses on identifying avenues of approach in cyberspace, long-range fires, air, and the electromagnetic spectrum.

3-105. Expeditionary signal company teams generally do not get to decide command post locations. However, once a command post is established, a decision can be made for mission effectiveness.

3-106. Mobility corridors are classified based on the distance between the terrain features that form the corridor. Though their ranges are not absolute, mobility corridors reflect the relative and approximate distance between terrain features. For more information on mobility corridors, refer to ATP 2-01.3.

3-107. Defensive considerations the commander can include in an evaluation of avenues of approach include—

- Likely enemy avenues into the rear area.
- How the enemy can use each avenue of approach.
- Site defensive plans and escape routes for signal sites.

Key Terrain

3-108. *Key terrain* is an identifiable characteristic whose seizure or retention affords a marked advantage to either combatant (ADP 3-90). Identification of key terrain is a conclusion, usually arrived at after enemy analysis and development of the plan, rather than by direct observation.

3-109. A prominent hilltop overlooking an avenue of approach may or may not be key terrain. Clear observation and fields of fire means little if the enemy can easily bypass it. However, if it offers cover and concealment, observation, and good fields of fire on multiple avenues of approach, or is on the only avenue of approach, then it offers a definite advantage to whoever controls it.

3-110. *Decisive terrain* is key terrain whose seizure and retention are mandatory for successful mission accomplishment (ADP 3-90). Some situations have no decisive terrain.

3-111. Commanders look at the tactical considerations in analyzing key terrain and consider—

- Which terrain the higher headquarters has identified as key terrain.
- Whether the terrain supports terrain masking to prevent the enemy detecting friendly communications nodes.
- Whether the terrain affects employment of communications nodes.

Military Aspects of Weather

3-112. The military aspects of weather are—

- Visibility.
- Winds.
- Precipitation.
- Cloud cover and ceiling.
- Temperature and humidity.
- Atmospheric pressure.
- Space weather

3-113. Commanders determine how the weather will affect the visibility, mobility, and survivability of the company and that of the enemy. Commanders also consider the effects of terrestrial and space weather on communications support.

> ***Note.*** Commanders determine how weather affects the persistence, spread, and enemy employment decisions of chemical, biological, radiological, and nuclear hazards. Refer to FM 3-11 for more information about chemical, biological, radiological, and nuclear operational effects.

Visibility

3-114. Commanders identify critical conclusions about visibility factors such as light data, fog, smog, smoke, dust, and heavy precipitation. They consider light data and identify critical conclusions about beginning of morning nautical twilight, sunrise,

sunset, end of evening nautical twilight, moonrise, moonset, and percentage of illumination. Some additional visibility considerations include—

- How the company can take advantage of limited illumination.
- How visibility will affect enemy target acquisition.
- Whether certain parts of the company's assigned area are prone to fog at certain times of the day or times of the year.

Winds

3-115. Windblown sand, dust, rain, or snow can reduce the effectiveness of radar and communications systems. Signal systems, especially large antennas, may suffer adverse effects from high winds. Some antenna systems require extra guy wires, supports, and anchor stakes to withstand heavy wind loading. Windblown sand and grit can damage electrical wire insulation over time or clog the environmental control units common on signal assemblages.

3-116. Wind is described as from ___ to ___ as in winds are from the east moving to the west. The leader must determine—

- Whether wind speed and direction will affect the employment of antenna masts or SATCOM antennas.
- Whether wind speed will cause obscurants to dissipate quickly.
- Whether the unit is downwind of chemical, biological, radiological, and nuclear contamination.

Precipitation

3-117. Precipitation includes rain, sleet, snow, and hail. Precipitation affects soil trafficability, visibility, and optical systems. Heavy precipitation can reduce the quality of supplies in storage. Heavy rain or snow cover can reduce the efficiency of many communications systems, operating at higher frequencies, including SATCOM and high throughput line of sight systems through rain fade. Precipitation considerations include—

- Exposure of electrical equipment.
- The use of higher frequency bands such as C, X, and Ku and the effects of rain fade on each.
- How precipitation, or lack of precipitation, will affect the mobility of the unit or of enemy forces.
- Specific locations in the assigned area that the company should avoid during times of increased precipitation, due to flooding, mud slides, or extremely loose soil.
- Specific portions of a convoy route that may be susceptible to freezing or black ice due to precipitation.

Cloud Cover

3-118. Heavy cloud cover that obscures at least 5/8ths of the sky is known as a ceiling. Ceilings may degrade target acquisition systems, infrared guided munitions, SATCOM, and general aviation operations. Some types of clouds reduce the effectiveness of SATCOM systems. Clouds may reflect, absorb, scatter, diffract, or refract radio waves.

3-119. Cloud cover affects different frequencies of radio waves to greater or lesser extent. As an example, extremely high frequency and super high frequency SATCOM signals suffer much greater signal loss through heavy cloud cover than systems that operate at lower frequencies. Heavy cloud cover may reduce the performance of SATCOM systems. Cloud cover considerations include—

- How cloud cover will affect satellite transport.
- Time periods during which cloud cover will reduce the effectiveness of communications equipment.

Temperature and Humidity

3-120. Extreme shifts in temperature and humidity reduce personnel and equipment capabilities and may require the use of special shelters or equipment. Air density decreases as temperature increases and increases as humidity increases. The leader identifies critical factors about temperature, including high and low temperatures and the effects of obscurants and chemical, biological, radiological, and nuclear agents. Temperature and humidity considerations include—

- How temperature and humidity will affect the team and equipment.
- Whether temperatures and humidity favor the use of non-persistent chemical, biological, radiological, and nuclear agents.
- How extreme heat or extreme cold will affect battery life in handheld devices, such as radios and optics.

Atmospheric Pressure

3-121. Atmospheric pressure can have significant effects on military operations, affecting communications systems by causing radio waves to bend, due to atmospheric ducting. It may also significantly impact aviation operations, including those of unmanned aircraft systems. Based on the elevation of the assigned area, atmospheric pressure may affect the lift capacity of aircraft requiring alternate transportation. At higher altitudes or in low-pressure environments, the reduced air density can decrease the lift generated by rotary wing aircraft, limiting load capacity for operations like—

- Air deployment of systems.
- Aerial resupply.
- Medical evacuation.

Space Weather

3-122. *Space weather* is the conditions and phenomena in space and specifically in the near-Earth environment that may affect space assets or space operations (JP 3-59). Geomagnetic storms can cause radar interference, radar propagation anomalies, and satellite-based position, navigation, and timing errors, critical to signal systems. Most space weather phenomena are predictable. Higher echelon space officers can advise of projected space weather effects on communications. Refer to FM 3-14 for detailed information about space weather phenomena. Analysis of Troops and Support Available

3-123. Commanders realistically and objectively study their company to determine the number, type, capabilities, and condition of available friendly troops and other available support. Analysis of troops and support determines what assets will be available to

accomplish the mission and the combat potential of the unit. The commander attempts to determine—

- The strengths and weaknesses of subordinate leaders.
- The supply status of class I, III, and V and other necessary items.
- The present physical condition of the company—health, morale, and sleep.
- The condition of assigned company equipment.
- The unit's training status and experience relative to the mission.
- Additional assets required to accomplish the mission.

Analysis of Time Available

3-124. Commanders visualize their company in time and space. As events occur, the commander adjusts the time available to the company and assesses its impact on the mission. Understanding how long it takes to execute a task helps determine where the company will be upon completion of that task. The commander must consider—

- Overall time available.
- Priorities of work to be accomplished, including security, maintenance, resupply, coordination, rehearsals, inspections, and sleep.
- Planning and preparation.
- Times specified by the commander in the OPORD for such activities as reconnaissance, rehearsals, and logistics package operations.
- Time required on station.
- Time required for movement to deployed location (convoy, rail, air, or sea).

3-125. Commanders conduct reverse planning to ensure the company can accomplish all specified, implied, and essential tasks in the time available. They develop a reverse planning timeline, beginning with actions on the objective and working backward through each step of the operation and preparation to the present time.

Analysis of Civil Considerations

3-126. *Civil considerations* are the influence of manmade infrastructure, civilian institutions, and attitudes and activities of the civilian leaders, populations, and organizations within an assigned area on the conduct of military operations (ADP 6-0). Civil considerations of the operational environment either help or hinder friendly or enemy forces. The difference lies in taking the time to learn the situation and its possible effects on the operation. Factors in analysis of civil considerations include—

- How civil considerations will affect the operation of signal sites.
- How the signal systems used might affect civilian communications and electronic devices.

3-127. The supported unit provides the company an analysis of civil considerations that affect the mission. The mnemonic used to analyze and describe these civil considerations is areas, structures, capabilities, organizations, people, and events. Refer to ATP 2-01.3 for more information about civil considerations.

RISK ASSESSMENT

3-128. *Risk assessment* is the identification and assessment of hazards (first two steps of the risk management process) (JP 3-26). Leaders at all levels manage risk to protect the

force and aid in mission accomplishment. The commander identifies risks based on the results of mission analysis. Leaders conduct continual risk assessment throughout the duration of the mission.

3-129. Once leaders identify risks, they attempt to mitigate or eliminate those risks through the use of controls. The commander establishes the overall risk tolerance level for the mission. Leaders determine in their plan how to reduce risk to an acceptable level. For example, leaders may mitigate the risk of fratricide by taking into consideration surface danger zones and risk estimate distances, resulting in the emplacement of target reference points and phase lines used to control maneuver and thus reduce this risk. Refer to ATP 5-19 for more information on the risk management process.

DEVELOP THE PLAN AT THE COMPANY LEVEL

3-130. The commander provides a course of action to the company. The company commander determines how to accomplish assigned tasks while meeting the battalion commander's intent.

3-131. The commander begins to develop a plan that is—

- **Suitable**—must accomplish the given task.
- **Feasible**—is executable given the skills, time, and resources on hand.
- **Acceptable**—the military advantage gained justifies the expected cost.
- **Distinguishable**—differs sufficiently from other approaches (if required) considered to achieve the given task.
- **Complete**—fully addresses who, what, where, when and how, from start to finish.

3-132. Commanders may be able to accomplish the given task and purpose in more than one way. They consider tactics, techniques, and procedures from doctrinal publications, unit SOPs, history, lessons and best practices, or other resources to determine whether a solution to a similar tactical problem already exists. Commanders can determine what combinations of personnel and systems they need to accomplish their assigned tasks. This is known as assigning troops to task and is based on the mission variables of METT-TC (I) the leader faces.

3-133. Commanders identify the best ways to use the available terrain to mitigate the enemy's ability to detect and locate friendly transmissions. This can be achieved through terrain masking involving the use of natural or artificial features to conceal or disrupt transmissions.

3-134. Commanders ensure the deployed communication package can accomplish mission. Commanders solidify the plan by notionally fighting it against how they believe the enemy will operate. Asking what if throughout the process can help identify points of friction not previously considered.

3-135. This process may be done solely by commanders who review the plan up to that point, or by including the first sergeant, platoon leaders, platoon sergeants and other subordinate leaders' input. This enables the commander to—

- Anticipate events in the assigned area.
- Determine conditions and additional resources required for success.

- Identify additional control requirements.
- Identify friendly coordination requirements.
- Appreciate the time, space, and triggers needed to initiate signal site displacement.
- Project sustainment requirements.
- Determine defense requirements for signal sites and coordinate with nearby units for support.
- Complete paragraphs three, four, and five of the OPORD.

STEP 4 – INITIATE MOVEMENT

3-136. Commanders initiate movements necessary to continue mission preparation or to posture the unit for starting the mission. This step can be executed any time during the sequence of troop leading procedures. It can include execution of priorities of work; movement to an assembly area, battle position, or a new assigned area; or the movement of guides or quartering parties.

STEP 5 – CONDUCT RECONNAISSANCE

3-137. Signal site reconnaissance involves representatives from the supported unit G-3 or S-3 and key signal leaders. The reconnaissance team should ensure all key leaders from the company and platoons participate in site reconnaissance and maintain continuous radio communication. The proposed site should be large enough to accommodate all signal assemblages and support equipment.

3-138. Leaders must ensure the site is defensible and offers adequate escape routes to prevent overrun by an enemy force. They should also consider how well the site is concealed from major roads or other vantage points and how the site's natural terrain can support terrain masking to prevent enemy direction finding. Refer to FM 6-02 for more information about site selection and reconnaissance.

STEP 6 – COMPLETE THE PLAN

3-139. Commanders refine their plan, prepare analog and digital overlays, complete sustainment requirements, and update the tentative plan based on the latest reconnaissance. Commanders prepare briefing sites and other briefing materials they might need to present the OPORD directly to their company. Based on the unit SOP and to maximize use of time, other members of the platoon may prepare graphics, overlays, briefing sites, or briefing materials.

3-140. Using the five-paragraph OPORD format helps commanders explain all aspects of the operation:

- Situation.
  - Terrain.
  - Enemy.
  - Higher and adjacent friendly units.
- Unit mission.
- Execution.
- Sustainment.
- Command and signal.

3-141. The OPORD format serves as a checklist to ensure coverage of all relevant details of the operation. Ultimately, the plan should be as simple as possible, while at the same time ensuring the company's signal support plan supports the battalion commander's intent.

STEP 7 – ISSUE THE ORDER

3-142. The OPORD precisely and concisely explains the commander's concept of how the company will accomplish its mission. The commander delivers the OPORD quickly, with confidence, and in a manner that allows subordinates to concentrate on understanding the commander's vision, not just repeating what is said verbatim.

3-143. Whenever possible, commanders issue the order in person. They look into the eyes of their subordinate leaders to ensure each one understands the mission and what the supported unit must achieve. If commanders already addressed an item adequately in a previous WARNORD, they simply state no change or provide necessary updates. Ultimately, the commander briefs the OPORD in the most effective manner to convey information to subordinates.

3-144. Commanders complete the order with a confirmation brief. At a minimum, platoon leaders and platoon sergeants should be able to backbrief the company's mission and intent, the company commander's intent, their own tasks and purpose, and when they will inform their teams of the mission details if they were not present at the OPORD brief. The confirmation brief provides an opportunity to identify or highlight issues or concerns. Figure 3-4 on page 68 outlines the five-paragraph OPORD format.

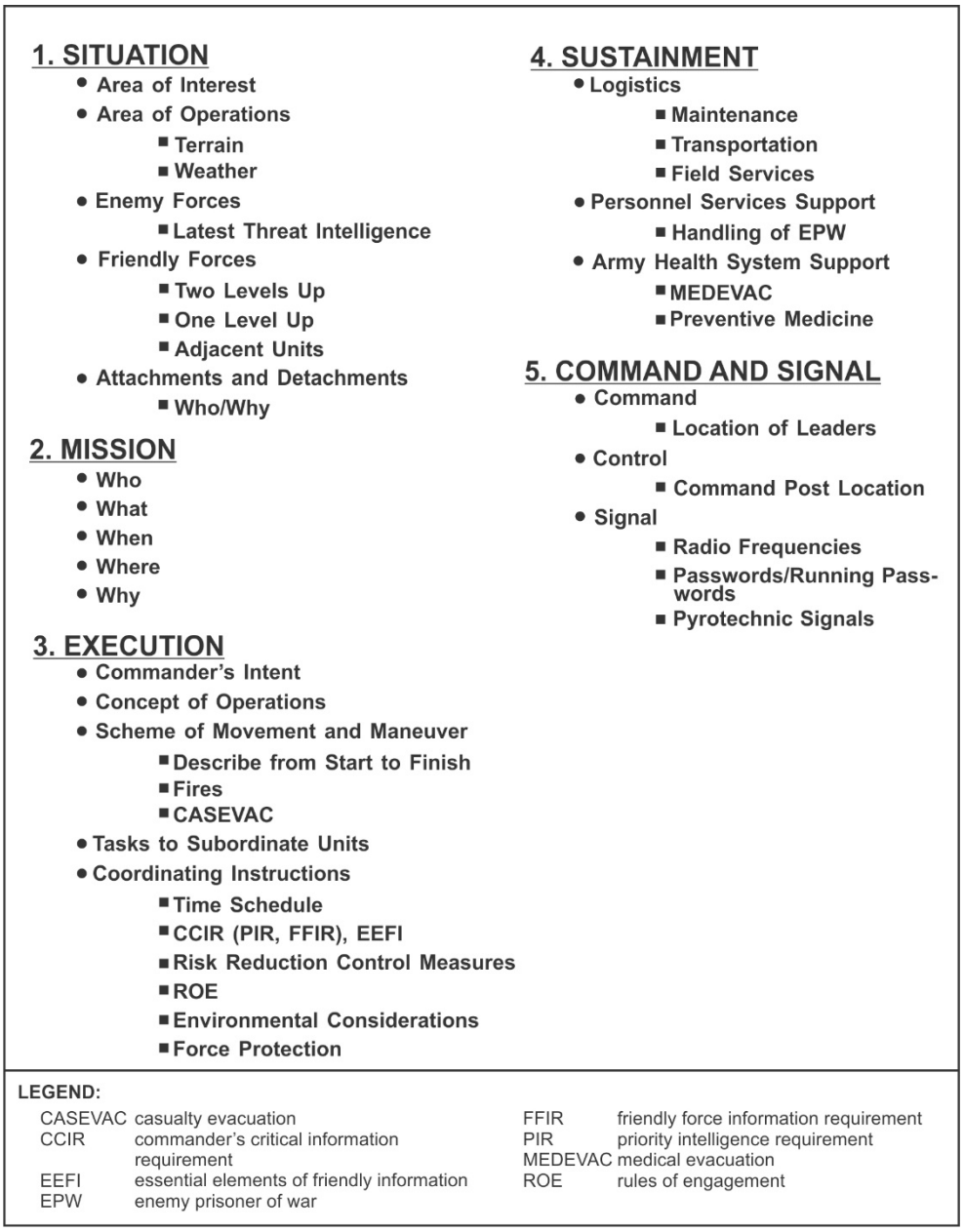


Figure 3-4. Operation order format

STEP 8 – SUPERVISE AND REFINE

3-145. After issuing the OPORD, the commander must ensure the required activities and tasks are completed quickly before mission execution. Supervision is the primary

responsibility of all leaders. Commanders check those items or events deemed important for mission accomplishment. This includes—

- Conducting backbriefs on all aspects of the mission.
- Observing rehearsals.
- Inspecting load plans to ensure teams carry what is necessary for the mission or what the OPORD specifies.
- Inspecting the status and serviceability of weapons and communications systems.
- Inspecting maintenance activities.

ABBREVIATED TROOP LEADING PROCEDURES

3-146. When there is not enough time to conduct all eight steps of troop leading procedures in detail, such as when a change of mission occurs after an operation is in progress, the commander truncates the troop leading procedures to save time. The commander follows most steps of abbreviated troop leading procedures mentally but skips none of the steps.

3-147. Once the order is received, the commander conducts a quick map reconnaissance, analyzes the mission variables of METT-TC (I), and contacts the platoon leaders. The platoon leader ensures the team leaders post the minimum required control measures on their maps and issues a FRAGORD that covers the key elements of the enemy and friendly situations, the platoon mission, and the concept of operations. The FRAGORD may omit the sustainment and command and signal paragraphs if they are unchanged or covered by a tactical SOP. The platoon leader and team leaders may also conduct a quick walk-through rehearsal of critical elements of the support plan using a hastily prepared terrain model or sand table.

3-148. In some cases, there may not be enough time even for these shortened procedures. The company may have to move out and receive FRAGORDs by radio or at the next scheduled halt. In this case, it becomes critical for the commander to send company FRAGORDs to the platoon leaders explaining the company's purpose within the overall plan.

3-149. Other keys to success when abbreviated troop leading procedures are in effect include a well-trained company; clearly developed, thoroughly understood SOPs; and an understanding by all supporting members of the supported unit of the current tactical situation.

SECTION IV – REHEARSALS

3-150. Rehearsals are practice sessions conducted to prepare units for an upcoming operation or event and the most valuable tool in preparing the company for the upcoming operation. Effective rehearsals require platoons to perform required tasks, ideally under conditions as close as possible to those expected for the actual operation. Participants maneuver their actual vehicles or use vehicle models or simulations while interactively verbalizing their elements' actions.

3-151. The PACE plan helps ensure the maneuver unit can continue to communicate if its primary means of communication fails. Units should rehearse and validate the PACE

plan during mission and communication rehearsals to ensure the alternate, contingency, and emergency means of communication are viable and that all personnel understand the triggers and can execute the plan as necessary.

3-152. Rehearsals should include crew drills such as—

- Medical evacuation requests.
- Requests for indirect fire support.
- Contingency actions.
- Actions on contact.
- Reaction to electromagnetic interference.
- COMSEC compromise.
- Emergency destruction.

3-153. Contingency plans should cover—

- Vehicle breakdowns.
- Lost vehicles.
- Accidents.

3-154. In a company-level rehearsal, the commander selects the tasks to rehearse and controls execution of the rehearsal. The commander may designate a subordinate leader to role-play the enemy they anticipate facing during the operation.

Note. A rehearsal is different from the process of talking through a plan. For example, in a rehearsal, platoon sergeants send a complete spot report when reporting enemy contact, rather than simply saying, I would send a spot report now.

REHEARSAL PURPOSES

3-155. Commanders use well-planned, efficiently run rehearsals to—

- Reinforce training and increase proficiency in critical tasks.
- Reveal weaknesses or problems in the plan.
- Synchronize the actions of the signal teams.
- Confirm coordination requirements between the company and adjacent units.
- Improve each company member's understanding of the concept of the operation, the signal support plan, anticipated contingencies, and possible actions and reactions for various situations that may arise during the operation.

REHEARSAL TYPES

3-156. The commander can choose among several types of rehearsals, including—

- Backbriefs.
- Combined arms rehearsals.
- Support rehearsals.
- Battle drill or SOP rehearsals.
- Communications rehearsal.

BACKBRIEF

3-157. A backbrief is a briefing by a subordinate leader to the commander to review how each intends to accomplish their respective portions of the mission. Normally, subordinates perform backbriefs throughout preparation. Backbriefs allow commanders to clarify the mission early in subordinate planning and identify any problems in the concept of operations. The commander conducts backbriefs after platoon leaders have had a chance to review the OPORD but before the company rehearsal begins.

COMBINED ARMS REHEARSAL

3-158. A combined arms rehearsal is a rehearsal in which subordinate units synchronize their plans with each other and is normally conducted at company-level and above. If they participate in a combined arms rehearsal, commanders generally brief their task and purpose, composition, disposition, and key actions executed by phase, though the exact information briefed varies by unit SOP.

SUPPORT REHEARSAL

3-159. The support rehearsal helps synchronize each warfighting function with the overall operation. Commanders may take part in the support rehearsal depending on their task and purpose and how it relates to the higher headquarters' operation.

BATTLE DRILL OR STANDARD OPERATING PROCEDURE REHEARSAL

3-160. Battle drills are collective actions performed without the application of a deliberate decision-making process. A battle drill is initiated on a cue, such as an enemy action or a leader's command. Cybersecurity incident response for network intrusion or SATCOM restoration battle drills can be used to train Soldiers. A battle drill is a trained response to a given stimulus. Battle drills require minimal leader orders to accomplish. Synchronization and reaction speed are enhanced when battle drills are identified, and the required reactions are defined in the unit SOP and rehearsed during training.

3-161. A battle drill or SOP rehearsal ensures all participants understand a technique or a specific set of procedures. Throughout preparation, signal teams rehearse battle drills and SOPs. These rehearsals do not require a completed order from the company to execute. Commanders place priority on drills for actions they anticipate occurring during the operation. Refer to FM 6-0 for more information about battle drills.

COMMUNICATIONS REHEARSAL

3-162. A communications rehearsal is a planned test of all the communication platforms used in a command post. This test ensures that operators are well-versed with their systems, understand their capabilities and limitations, and are fully prepared to conduct operations. The communication rehearsal also helps signal personnel and the command post warfighting functions to verify their systems' data information flow, switch and router configurations, and the availability and functionality of all systems in the unit's communication PACE plan. It also ensures that all personnel understand the triggers to switch from one means of communication to another. PACE rehearsals can help ensure backup communication methods are seamless and functional. Emission control rehearsals can also be conducted to ensure the unit's ability to operate with a minimized

electromagnetic signature. See paragraph 4-25 for more information on emission control. Refer to FM 6-0 for more information about communications rehearsals.

METHODS OF REHEARSALS

3-163. Rehearsals should follow the crawl-walk-run methodology whenever possible, see figure 3-5. This prepares the company for increasingly difficult conditions. Refer to FM 6-0 for more information on rehearsals. Security must be maintained; however, units can conduct these forms of rehearsals if mission variables permit:

- Full-dress rehearsal.
- Key leader rehearsal.
- Terrain-model rehearsal.
- Digital terrain-model rehearsal.
- Sketch-map rehearsal.
- Map rehearsal.

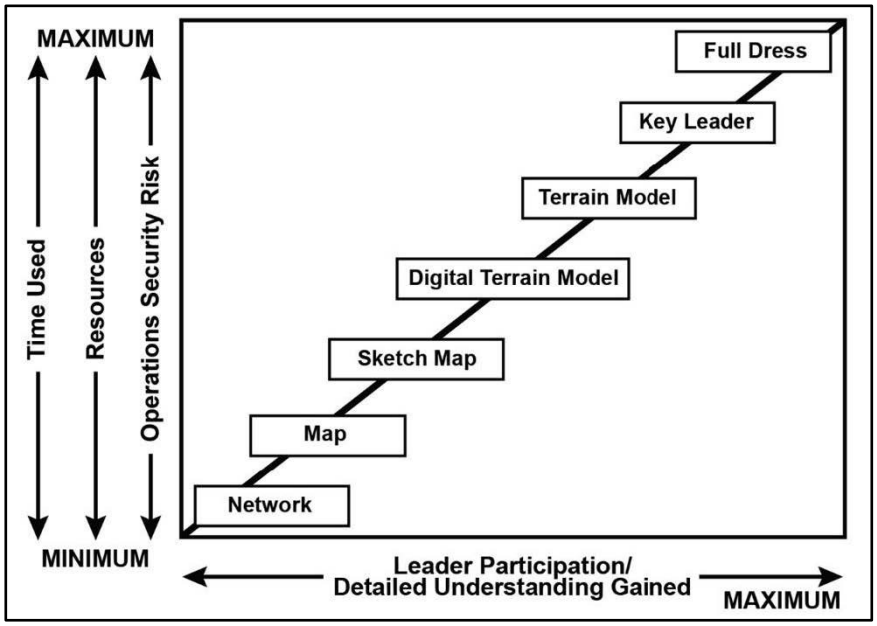


Figure 3-5. Methods of rehearsals

FULL-DRESS REHEARSAL

3-164. A full-dress rehearsal includes every participating company member and system, executed on terrain similar to the assigned area, initially under good light conditions, and then in limited visibility. Any attachments to the company take part in this rehearsal, bringing with them any equipment they need to execute the mission.

REDUCED-FORCE (KEY LEADER) REHEARSAL

3-165. This rehearsal involves only key leaders of the organization and subordinate units and normally takes fewer resources than a full-dress rehearsal. Terrain requirements

mirror those of a full-dress rehearsal. A reduced-force (key leader) rehearsal can be used to prepare key leaders for a full-dress rehearsal.

TERRAIN-MODEL REHEARSAL

3-166. The terrain-model rehearsal is the most popular rehearsal technique. A terrain-model rehearsal takes far less time and fewer resources than a full-dress or reduced-force (key leader) rehearsal. This technique employs an accurately constructed model to help subordinates visualize the mission. When possible, the commander places the terrain model near, or where it overlooks, the actual terrain of the assigned area. The model should be large enough to depict graphic control measures and important terrain features for reference and orientation. The company should take care to conceal the terrain model from enemy air assets.

DIGITAL TERRAIN-MODEL REHEARSAL

3-167. During a digital terrain-model rehearsal, units drape high-resolution imagery over elevation data, creating a fly-through or walk-through of the mission. The model may link graphics, detailed information, unmanned aircraft systems, and ground imagery to key points to provide accurate insight to the plan.

SKETCH-MAP REHEARSAL

3-168. Sketch-map rehearsal procedures are similar to those for the terrain-model rehearsal. The sketch must be large enough to allow all participants to see as each subordinate walks through an interactive oral presentation of their actions. Platoons can use symbols to represent their signal team locations and maneuver on the sketch and use complete radio transmissions when executing their movements.

MAP REHEARSAL

3-169. Procedures for a map rehearsal are similar to those for the sketch-map rehearsal, except the leader uses a map and operation overlay of the same scale as the commander used to plan and control the operation. This technique is useful in conjunction with a confirmation brief or backbrief involving subordinate leaders.

PRE-COMBAT CHECKS AND INSPECTIONS

3-170. The platoon leader or platoon sergeant observes each team during preparation for combat. They conduct pre-combat checks and inspections once the team leaders report their teams and vehicles are prepared. It is understood that platoon leaders will check items they deem critical for the upcoming operations, but the team leaders check all items based on the unit tactical SOP. Failure at the team leader level to check all systems-not just the ones the platoon leader inspects personally-could lead to a critical element or piece of equipment failing during operations.

PRE-COMBAT CHECKS

3-171. Pre-combat checks differ from pre-combat inspections in that they are quick combat checks performed at team-level designed to account for individuals and equipment. Pre-combat checks do not require formal advance notification. They are designed to be quick and concise, verifying the teams have all necessary equipment to accomplish their mission. Examples for signal pre-combat checks include—

- Signal team checks.
- COMSEC.
- Fill devices.
- Courier cards.
- Changeover times.
- Radio checks and communications cards.
- Fuel level in vehicles and generators.
- Military vehicle driver's licenses.
- Maps and overlays of the assigned area.
- Ammunition checked and stored properly.
- Vehicles uploaded according to the unit tactical SOP.
- Teams' uniforms and equipment necessary to accomplish the tasks are accounted for.

Note. The standardization of load plans allows leaders to quickly check accountability of equipment. It also ensures standard locations of equipment in each vehicle.

PRE-COMBAT INSPECTIONS

3-172. Pre-combat inspections allow the platoon leader to check the platoon's operational readiness. The key goal of a pre-combat inspection is to ensure that teams and communications systems are fully prepared to execute the upcoming mission. The platoon leader includes the time and location for pre-combat inspections in the platoon OPORD, reinforcing their importance and ensuring they occur as part of pre-mission preparation.

3-173. It is essential that the entire company chain of command know how to conduct pre-combat checks and pre-combat inspections according to applicable SOPs. Examples of an inspection include—

- Perform before-operation preventive maintenance checks and services and report or repair deficiencies, if necessary.
- Ensuring spare equipment is available and functional.
- Perform communications checks of voice and digital systems.
- Inspect and verify maps and corresponding analog and digital graphics.
- Ensure teams understand the plan and are in the correct uniform and mission oriented protective posture based upon the threat level.
- Determine types of ammunition the mission requires.
- Review the supply status of rations, water, fuel, oil, ammunition, pyrotechnics, first-aid kits, and batteries for such items as flashlights, night vision devices, and chemical, biological, radiological, and nuclear equipment.
- Ensure vehicles and communications assemblages are correctly camouflaged to match the assigned area.

SECTION V – RECOVERY

RECOVERY

3-174. Recovery should be conducted in accordance with the unit SOP based on mission, equipment and other factors dictated by the commander. Recovery generally revolves around a daily schedule to be completed before the end of each day.

3-175. The recovery process is established to ensure the unit can redeploy quickly and efficiently. Recovery operations should be conducted to standard after every training event and mission. The recovery process does not have to go through multiple days. Daily recovery operations can be scheduled according to the mission timelines set by the commander. An example template includes—

- **Day 0**
  - Conduct accountability of all sensitive items.
  - Remove personal gear from vehicles and free of loose debris.
  - Clean vehicle windows, mirrors, and lights.
- **Day 1**
  - Conduct after operation preventive maintenance checks and service on all vehicles, trailers, and generators.
  - Inventory basic issue items.
  - Clean and service weapon systems.
  - Clean vehicles on a wash rack.
  - Conduct inventory and replenish individual first aid kits, combat lifesaver bags, and vehicle first aid kits.
- **Day 2**
  - Conduct signal maintenance, ensuring all systems are verified working, communications-electronics maintenance is conducted, and maintenance personal are notified of any issues.
- **Day 3**
  - The commander inspects unit vehicles and equipment.

This page intentionally left blank.

Chapter 4

Support to Operations

This chapter defines the various command posts and describes the common functions of all command posts. A discussion of the types of command posts by echelon and unit follows. Next, the chapter provides considerations for effective command posts organization and employment from a communications perspective of an expeditionary signal company.

RECEPTION, STAGING, ONWARD MOVEMENT, AND INTEGRATION

4-1. Expeditionary signal companies generally arrive in a partially established theater supporting reception, staging, onward movement, and integration. Peer threats could complicate reception, staging, onward movement, and integration. Leaders should continuously evaluate the environment while supporting the reception, staging, onward movement, and integration of forces into theater. Leaders can conduct enroute mission planning prior to reception, staging, onward movement, and integration utilizing Command and Staff Palletized Airborne Node teams. See paragraph 2-65 for more information on the Command and Staff Palletized Airborne Node teams.

4-2. The four steps of reception, staging, onward movement, and integration are—

- **Reception**—the process of unloading personnel and materiel from strategic transport, marshaling the deploying units, transporting them to staging areas, if required, and providing life support to deploying personnel.
- **Staging**—the process of assembling, holding, and organizing arriving personnel and equipment into units and forces, incrementally building combat power, and preparing units for onward movement, and providing life support for the personnel until the unit becomes self-sustaining.
- **Onward Movement**—the process of moving units and accompanying materiel from reception facilities and staging areas to tactical assembly areas or other theater destinations, moving arriving non-unit personnel to gaining commands, and moving arriving sustainment materiel from reception facilities to distribution sites.
- **Integration**—the synchronized transfer of authority over units and forces to a designated component or functional commander for employment in the theater of operations.

COMMAND POST SUPPORT

4-3. A *command post* is a headquarters, or a portion thereof, organized for the exercise of command and control (FM 6-0). Often divided into echelons, each echelon of the headquarters is a command post, regardless of whether the commander is present.

4-4. Command posts contain vital systems for the command and control warfighting function. They also provide military leaders with the capability to make timely decisions, communicate those decisions to subordinate units, and monitor the execution

of these decisions. Expeditionary signal company teams directly support the command posts' ability to conduct command and control functions.

OVERVIEW

4-5. Command post functions directly relate to assisting commanders in understanding, visualizing, describing, directing, leading, and assessing operations. Different types of command posts, such as the main command post or the tactical command post, have specific functions by design.

Note. Refer to ATP 6-0.5 for a detailed discussion of command post administration.

COMMAND POST SURVIVABILITY

4-6. Command post survivability is vital to mission success. Depending on the threat, command posts need to remain small and highly mobile, especially at lower echelons. Command posts are easy for enemies to locate and target when concentrated. Additional measures include cover or shielding by terrain features or urban structures. The considerations in this section apply to command posts at all echelons.

4-7. Commanders should review the protection warfighting function continually and refine training objectives for peer threats. Refer to ADP 3-37 for more information on detecting, preventing, and mitigating threats and hazards. Commanders should implement current lessons and best practices from across the force to better employ the company during command post support. Methods to enhance command post survivability include—

- Dispersion.
- Frequent displacement and mobility.
- Size.
- Redundancy.
- Signature management.
  - Visual.
  - Radar.
  - Infrared (thermal).
  - Noise.
  - Electromagnetic.

Note. See appendix A for techniques to mitigate the various command post signatures.

Dispersion

4-8. Dispersing command posts enhances the survivability of the command and control system. Commanders should place the minimum necessary resources in the close area forward and locate larger facilities in the rear area. This makes it harder for enemies to find and attack critical command and control nodes. It also decreases forward support and security requirements to protect command post capabilities.

4-9. Company elements could potentially operate within both the support and close area forward depending on the operation. Commanders should establish a plan of action in the event of combat loss of signal assets and consider which communication packages in the assigned area can support combat operations forward.

Frequent Displacement and Mobility

4-10. Maintaining continuity during displacement of a command post or catastrophic loss requires designating alternate command posts and passing control between command posts. (ATP 6-0.5) Command post displacement requires advance coordination and battle handover so at least one command post is always available to control the fight.

4-11. Command post mobility is important, especially at lower echelons during combat operations. Lower-echelon command posts and those employed forward in the close area may need to move quickly and often. Small size and careful planning enable rapid and effective command post displacement.

4-12. Signal teams train for frequent displacement and high mobility through—

- Battle drills.
- Timed crew drills.
- Team training and certification.

Size

4-13. The size of a command post affects its mobility and survivability. Large command posts may increase capacity and enhance face-to-face coordination and collaboration, but their size makes them vulnerable to multiple means of acquisition and attack. Smaller command posts are easier to protect but may not have the capacity to control operations effectively.

4-14. Large command post nodes are much larger and more difficult to assemble. Teams should take appropriate measures to expedite the movement of equipment by proactively consolidating equipment and recovering all non-critical equipment not in use prior to command post movement to a new location.

Redundancy

4-15. Reducing command post size reduces detectability and enhances mobility. However, some personnel and equipment redundancy are necessary to maintain continuous operations. During periods of high operational tempo, personnel and equipment are subject to combat loss and failure due to stress. The right amount of redundancy allows command posts to continue to operate effectively.

4-16. The commander should ensure that all redundant links such as line of sight systems are employed, when possible, to supplement beyond line of sight systems due to outages caused by enemy fire or malfunction. The PACE plan should include all tactical communication and power generation systems due to enemy fire or malfunction.

4-17. Redundancy should involve decentralized locations of redundant links so no one attack can destroy all transmission systems. Expeditionary signal company elements supporting command posts of any size should consider—

- Line of sight systems location relative to the command post.
- Beyond line of sight systems location relative to the command post.
- Whether line of sight or beyond line of sight systems are most appropriate based on the mission variables of METT-TC (I).

Command Post Signatures

4-18. Since World War II, the size and complexity of command posts have increased dramatically. Command post signatures have correspondingly increased with the number and types of vehicles and communications systems employed. All of these signatures increase an enemy's likelihood of successfully detecting and targeting critical command and control nodes.

Visual

4-19. Command posts require excellent camouflage and concealment to survive on the battlefield. Camouflage and concealment improve operations security and increase survivability by minimizing the observable size of command posts. Command post camouflage and concealment require reconnaissance, planning, discipline, security, and maintenance. Reconnaissance and heightened security patrols enhance camouflage and concealment efforts by denying access to vantage points from which an enemy can observe a command post.

4-20. Communications teams supporting the command post should have their own camouflage netting for each individual communications assemblage on hand. The camouflage should be pre-rolled and sized properly for expedited setup. Teams should train with camouflage during training events for teams to be proficient in site setup and recovery.

4-21. Defensive positions often create scarred earth signatures and detectable patterns due to earth excavation. While defensive positions are critical to command post survivability, units should mitigate the visual signatures of defensive positions by taking advantage of available natural cover and concealment. Planners should consider the following regarding camouflage and concealment for command posts—

- **Vehicle traffic**—carefully controlled traffic plans decrease the possibility of disturbing natural cover and creating new, observable paths.
- **Antennas—**antennas and numerous support towers are common to most command posts. Painting shiny surfaces of antennas and support equipment with anti-reflective, nonconductive green, black, or brown paint makes them harder to observe at distance.
- **Security emplacements**—barbed wire, physical barriers, security and dismount points, and other observable security measures can indicate command post operations.
- **Use of decoys**—decoys can be highly effective means of confusing the enemy target acquisition process, particularly against airborne sensors. High fidelity physical decoys provide a realistic electromagnetic signature to enemy detection devices such as radars.

Radar

4-22. Radio frequency reflective camouflage netting can help reduce the radar signature of command posts. Barbed wire exhibits a measurable radar cross section at radar frequencies. Emplacing barbed wire and concertina wire to follow natural terrain features, when possible, reduces their radar signatures.

Infrared (Thermal)

4-23. Power generators and other heat sources produce thermal signatures that enemy surveillance and target acquisition sensors can detect. Emplacing heat-producing equipment and other thermal sources in defilade positions, within structures or under natural cover mitigates their infrared signature. Heat diffusers that disperse and vent vehicle exhaust away from the threat direction, are an expedient means of thermal signature reduction.

Noise

4-24. Noise discipline contributes to command post survivability. The power generation equipment associated with signal equipment can generate significant noise. During site selection, signal leaders should consider measures to mask and diffuse noise and heat signatures such as—

- T-barriers.
- Sandbag emplacement.
- Buildings.

Electromagnetic

4-25. The cyberspace electromagnetic activities section at echelons brigade and above ensures the command post's electromagnetic signature is properly managed. Expeditionary signal companies should understand their electromagnetic signature in their area. It is the responsibility of individual command posts to manage their electromagnetic signature to mitigate threat detection. This can be achieved by practicing emission control (EMCON).

4-26. *Emission control* is the selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors, b. mutual interference among friendly systems and/or c. enemy interference with the ability to execute a military deception plan (JP 3-85). EMCON reduces the likelihood of detection by threat sensors and direction-finding systems and helps conceal the locations of friendly forces.

4-27. EMCON prevents the threat discovering and attacking the locations of friendly forces with long range fires and EW. When establishing EMCON best practices, it is important to understand the general categories and status criteria for EMCON conditions. Based on the tactical situation or operational environment, the commander can dictate the appropriate EMCON condition. Table 4-1 on page 82 outlines the five EMCON conditions and the general descriptive criteria associated with each condition.

Table 4-1. Emission control conditions

EMCON Condition	Description
EMCON 1 Green	Describes a situation where there is no apparent hostile activity against friendly emitter operations. *Operational performance of all EMS-dependent systems is monitored; password and encryption systems are used as a layer of protection.*
EMCON 2 Yellow	Describes an increased risk of attack after detection. *Increased monitoring of all EMS activities is mandated, and all Department of Defense end users must make sure their systems are secure, encrypted, power levels monitored, and transmissions limited. EMS usage may be restricted to certain emitters. Rehearsal for elevated EMCON conditions is ideal.*
EMCON 3 Amber	Describes when a risk has been identified. *Electromagnetic counter-countermeasures (encryption/frequency hop/directional antennas) on important systems are a priority, and the CEWO's alertness is increased. All unencrypted systems are disconnected.*
EMCON 4 Red	Describes when an attack has taken place, but the EMCON system is not at its highest alertness. *Non-essential emitters may be taken offline, alternate or contingency means of communication may be implemented, and modifications are made to standard lower EMCON configurations (power levels and antenna types).*
EMCON 5 Black	Describes when attacks are taking place based on use of the EMS. *The most restrictive electromagnetic protection methods are enforced. Any compromised systems are isolated from the rest of the network.*
LEGEND:	
CEWO	cyber electromagnetic warfare officer
EMCON	emission control
EMS	electromagnetic spectrum

4-28. Commanders should consider EMCON 3 (amber) as the baseline for operations in the field. Units should routinely execute transitions to EMCON 4 (red) and EMCON 5 (black) during conflict. Commanders, assisted by the CEWO, should carefully evaluate minimum required capabilities to support operations during more restrictive EMCON conditions and discontinue use of unnecessary systems. For more information on EMCON criteria refer to FM 3-12.

4-29. Command post signatures increase with the number and types of vehicles and communications systems employed. These signatures increase an enemy's likelihood of successfully detecting and targeting critical command and control nodes.

4-30. A large number of antennas, their electromagnetic emissions, and support towers are common in major command posts. If tactically feasible, units should use remote antenna placement to reduce the vulnerability of the command post to collateral damage if an enemy destroys the communications system. When evaluating electromagnetic signatures emitted by command posts, planners should consider concentrations of vehicles, wear, and track marks due to heavy traffic, and air traffic. Parking vehicles and aircraft away from command posts mitigates the concentrated electromagnetic signature.

4-31. Command posts conduct electromagnetic masking using electromagnetic decoys to protect the locations of critical nodes. *Electromagnetic masking* is the controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy electromagnetic support measures/signals intelligence without significantly degrading the operation of friendly systems (JP 3-85). Electromagnetic decoys used for masking radiate at higher energy levels than normal communications to hide real transmission from enemy electromagnetic support and signals intelligence capabilities. Refer to ATP 3-12.3 for more information about electromagnetic masking. See appendix A for EMCON techniques.

ORGANIZATIONS REQUIRING TACTICAL COMMUNICATIONS AUGMENTATION

4-32. This section discusses organizations that have organic tactical communications assets but may require communications support packages for augmentation. Communications support packages provide additional communications capabilities for connectivity to the DODIN-A.

OVERVIEW

4-33. Some organizations have organic tactical communications assets. When assigned a theater mission that requires communications support beyond the scope of its communications capabilities, an organization requests communications support using the request for forces process. If available, the combatant commander sources the required capability from theater available forces. If the required capability is not available in theater, FORSCOM meets those communications needs by designating an element from the globally available force pool to design and deploy a communications support package that meets the validated requirements.

Corps

4-34. A corps may be given an assigned area in theater during large-scale combat operations, yet not be designated as a joint task force headquarters or joint force land component command. In this instance, the joint force land component command or its subordinate Army forces headquarters will designate the corps' assigned area. A corps organizes its assigned area into three distinct areas during large-scale combat operations-close, deep, and rear areas.

4-35. The corps signal, intelligence, and sustainment company has enough organic communications assets to support the corps main and tactical command posts. The corps headquarters requires augmentation to provide tactical internet support for attached functional support brigades in the corps rear area. Support units protecting supply routes may require communications augmentation for assigned or attached battalions operating in the corps close and deep areas. The expeditionary signal companies in the corps signal brigade or the theater signal brigade support these requirements.

HOMELAND DEFENSE, HOMELAND SECURITY, AND HUMANITARIAN ASSISTANCE

4-36. Expeditionary signal support is often required for the homeland security, homeland defense, and humanitarian assistance missions. Expeditionary signal companies routinely deploy in support of these operations, working alongside interagency and non-governmental organizations to provide signal support.

4-37. The U.S. homeland is the physical region that includes the continental United States, Alaska, Hawaii, U.S. territories, and surrounding territorial waters and airspace. The United States Government employs all instruments of national power to continuously detect, deter, prevent, and defeat threats to the homeland. By law, the DOD is responsible for two missions in the homeland: defense support of civil authorities and homeland defense.

4-38. Army forces operating within the United States encounter very different operational environments than they face outside the nation's boundaries. Although many of the small-unit tasks remain the same, there are important differences in the conditions associated with them. Principally, the roles of civilian organizations and the relationships of military forces to federal, state, territorial, tribal, and local agencies are different. These pronounced differences warrant defining a different task set than offense, defense, or stability. Army forces provide support depending on specific circumstances dictated by law. Soldiers and Department of the Army civilians need to understand domestic environments so they can employ the Army's capabilities efficiently, effectively, and legally.

4-39. Leaders should be aware of the policy and legal considerations of these operations such as special considerations, the Posse Comitatus Act, intelligence activities, acquisition of open-source information, domestic use of unmanned aircraft systems and rules of engagement among others. Refer to JP 3-27 for more information on homeland defense, including specific laws, and constitutional limitations.

HOMELAND DEFENSE

4-40. *Homeland defense* is he protection of United States sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression or other threats as directed by the President (JP 3-27). The DOD executes homeland defense by detecting, deterring, preventing, and defeating threats from actors of concern as far forward from the homeland as possible.

4-41. The DOD is the lead federal agency for defending against traditional external threats or aggression and against external asymmetric threats that are outside of the scope of homeland security operations.

HOMELAND SECURITY

4-42. *Homeland security* is a concerted national effort to prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage and recover from attacks, major disasters, and other emergencies that occur (JP 3-27). Homeland Security missions consist of—

- Prevent terrorism and enhance security.

- Secure and manage our borders.
- Administer and enforce immigration.
- Safeguard and secure cyberspace.
- Ensure disaster resilience.

4-43. While the DOD may support homeland security missions, the Department of Homeland Security is the lead federal agency for homeland security on land, and the United States Coast Guard is the lead federal agency for maritime homeland security.

DEFENSE SUPPORT OF CIVIL AUTHORITIES

4-44. Army forces combine defensive and offensive capabilities to execute defense support of civil authorities missions. Most defense support of civil authorities missions support a designated national special security event. A *national special security event* is a designated event that, by virtue of its political, economic, social, or religious significance, may be the target of terrorism or other criminal activity (JP 3-28). Olympics, inaugurations, or state funerals are examples of national special security events.

4-45. While every domestic support mission is unique, four defining characteristics shape the actions of commanders and leaders in any mission. These characteristics are that—

- State and federal laws define how military forces support civil authorities.
- Civil authorities are in charge, and military forces support them.
- Military forces depart when civil authorities are able continue without military support.
- Military forces must document costs of all direct and indirect support provided.

4-46. Expeditionary signal support during defense support of civil authorities is similar to normal command post operations with the exception of the need for Commercial Coalition Equipment and operating within a civilian environment where units support various interagency partners, including the Federal Emergency Management Agency.

4-47. The use of Commercial Coalition Equipment during defense support of civil authorities allows civilians to bring their own devices and allows the use of wireless transmission of civilian Internet service to support recovery efforts if approved by the commander.

4-48. Quality of service measures ensure users do not access high-bandwidth websites during peak usage times or during daily information and changeover briefs. Commercial Coalition Equipment bandwidth is limited to tactical internet speeds and is uncensored. For more information on defense support of civil authorities, refer to ADP 3-28.

HUMANITARIAN ASSISTANCE

4-49. The DOD humanitarian assistance mission includes several programs conducted to build the capacity of partner nations to provide essential services or to meet basic human needs to ensure the well-being of the population. Armed Forces participation in humanitarian assistance may be limited in scope and duration and designed to supplement or complement the efforts of the host nation that has the primary responsibility for providing that assistance and may support other departments or agencies.

Communications

4-50. Foreign humanitarian assistance missions often rely on government agencies and nongovernment organizations. Signal teams provide connections to commercial telephone networks, military satellite channels, and conventional military command and control systems to support those organizations including military units involved with recovery efforts. Commercial communications systems can be used to coordinate with other departments and agencies, disseminate meeting schedules, deconflict resource movement, and track logistics flow.

4-51. COMSEC for non-classified communications is essential, particularly when connections are made to the DODIN. Communications systems planning should consider the termination or transition of U.S. involvement and the transfer of responsibility to other agencies such as the United Nations or non-governmental organizations. Frequency management will help allocate finite frequency resources. The assisted government (if functioning) may control frequency management. U.S. forces may not have exclusive use of frequencies.

Interoperability

4-52. Signal leaders identify communications equipment interoperability among all participants. It is likely civilian interagency partners, host-nation agencies, and multinational forces will have their own communications networks. These may include commercial-leased circuits and satellite services, as well as high-frequency radio equipment. Signal teams should be equipped with communications equipment that facilitates collaboration with all mission partners. The need for interoperability of communications equipment in foreign humanitarian assistance operations may also necessitate using unclassified communications.

4-53. U.S. federal military forces may face challenges in conducting operations via unclassified means to promote interorganizational coordination and synchronization. The use of classified and unclassified modes of communication are both necessary, as classified modes are routinely used to relay militarily significant information while unclassified modes are needed for communication with nonmilitary entities. For more information on foreign humanitarian assistance refer to JP 3-29.

MISSION PARTNER NETWORKS

4-54. A mission partner network is a part of the mission partner environment and is the communications network within the environment. This network is a secret-releasable network enclave that securely integrates mission partner systems using common information technology infrastructure, enterprise services, and architectures. Approved exchange standards and services enable interoperable information exchange. Refer to ATP 6-02.61 for information on the mission partner environment.

4-55. The mission partner environment integrates technological, procedural, and human domain solutions to facilitate fast, full, and accurate information exchange, process execution, and mission partners' unity of effort. The mission partner environment is facilitated by the mission partner network, a shared network that enables collaboration, rapid dissemination of data and information, and an ability to project decisions based on common situational awareness. When collaborating with mission partners, digital

liaisons fill in the gaps that alleviate human, procedural, and technological constraints. Refer to ATP 3-16.02 for information on sharing information with mission partners.

COMMAND AND SUPPORT RELATIONSHIPS

4-56. Command and support relationships provide the basis for unity of command and unity of effort in operations and are the basis for task-organizing. Task-organizing is the act of designing a force, support staff, or sustainment package of specific size and composition to meet a unique task or mission (ADP 3-0). Refer to FM 6-0 for more information on command and support relationships.

4-57. Nonorganic combat and sustainment assets can significantly enhance the company's capabilities. Nonorganic elements support the company, and teams under established command and support relationships.

4-58. Command relationships define superior and subordinate relationships between unit commanders. Command relationships unify effort and give the commander the ability to employ the company with maximum flexibility. Command and support relationships include—

- Organic.
- Assigned.
- Attached.
- Operational control.
- Tactical control.
- Technical control.

ORGANIC

4-59. Organic forces are those assigned to and forming an essential part of a military organization. The Army establishes organic command relationships through organizational documents such as tables of organization and equipment and tables of distribution and allowances.

ASSIGNED

4-60. Assigned units remain subordinate to the higher headquarters for extended periods, typically years. An example would be that expeditionary signal platoons are assigned to expeditionary signal companies.

ATTACHED

4-61. Attached units are temporarily subordinated to the gaining headquarters. The period of attachment may be lengthy, often months or longer. Attached units return to their parent assigned or organic headquarters when the reason for the attachment ends.

OPERATIONAL CONTROL

4-62. Operational control is inherent in combatant command (command authority) and may be delegated within the command. An expeditionary signal company or one of their teams that are under operational control of a higher headquarters can be reorganized as necessary to accomplish assigned tasks.

TACTICAL CONTROL

4-63. Tactical control is inherent in operational control. Placing an expeditionary signal company under tactical control allows a higher headquarters to direct the tactical use of the company but does not provide authority to change organizational structure or direct administrative and logistical support.

TECHNICAL CONTROL

4-64. Technical control is not a formally defined command relationship but describes the control relationship between a signal element and its controlling network operations and security center or other DODIN operations authority. Controlling authorities exercise technical control through technical channels. *Technical channels* are the chain of authority for ensuring the execution of clearly delineated technical tasks, functions, and capabilities to meet the dynamic requirements of Department of Defense information network operations (ATP 6-02.71). Technical channels generally parallel the chain of command, with each successive echelon's control authority exercising technical control on behalf of the commander.

SIGNAL TEAM SUPPORT

4-65. The commander and the platoon leader should be involved with the early planning of the mission. The team leader should be present during the planning process of the mission to ensure that they know both the mission and key leaders to better support their team during the mission.

4-66. The signal team should understand the expectations of the supported unit before the mission starts. The team leader briefs their team on what the mission is and from whom they will receive support functions. The supported unit G-6 or S-6 is the primary point of contact for the team, otherwise a point of contact should be identified before the start of the mission.

4-67. Before movement, team leaders should fully understand—

- The supported unit.
- The supported unit's expectations of the team.
- Technical data and COMSEC required to establish communications support.
- Who will provide Class I–X supplies.
- Who will provide motor maintenance support.
- Who will provide communications-electronics maintenance support.
- What spare equipment will likely be needed.

Chapter 5
Logistics and Sustainment

This chapter outlines maintenance and maintenance management in the company. It discusses two-level maintenance, communications-electronics maintenance and the logistics support provided to build and preserve operational readiness.

SECTION I – MAINTENANCE

5-1. Army organizations are required to establish SOPs and a maintenance management processes to sustain, repair, evacuate, and report maintenance readiness status of critical communication systems. Refer to FM 4-0 for more on maintenance support. The Cyber Lessons and Best Practices Website contains sample maintenance SOPs.

MAINTENANCE MANAGEMENT

5-2. Army organizations establish SOPs and maintenance management processes to sustain, repair, evacuate, and report readiness status of critical communication systems.

5-3. Communications-electronics maintenance must be a priority in the unit's battle rhythm. By carefully managing scheduled and demand maintenance on signal equipment, units maintain visibility of the mission readiness of critical communications systems. Scheduled maintenance follows the schedule in the maintenance allocation chart in the equipment technical manual. Demand maintenance, or fault repair, is the process used by operators and maintainers to restore equipment to full functionality.

5-4. A maintenance plan should be a signed unit policy at the battalion level or higher. The maintenance plan outlines the separation in maintenance responsibilities in the unit, establishes a schedule for performing preventive maintenance checks and services on signal equipment, and clarifies the procedures to elevate maintenance issues to the appropriate maintenance support activity. Commanders should develop a maintenance focus based upon current operational challenges and maintenance trends. A deliberate, consistent, and engaged effort by all leaders is crucial to an effective maintenance plan.

5-5. Communications-electronics maintenance ensures signal systems remain fully mission capable. Signal operators perform preventive maintenance checks and services according to the operator's technical manual as scheduled maintenance. When equipment requires demand maintenance, operators troubleshoot the system to isolate the fault. In most cases, identified faults require a replacement line replaceable unit to correct the problem. Defined procedures for spare replenishment ensure replacement stock levels are adequate. The supporting communications-electronics maintenance shop maintains signal system spares, other than those identified in the end item component list as on-board spares. To maintain accountability, maintenance personnel track signal system spares in Global Combat Support System-Army as shop stock.

LIFE CYCLE MANAGED SYSTEMS

5-6. Life cycle managed items are military equipment that follow a formal cycle associated with acquisition, development, production, fielding, sustainment, and final disposition. Life cycle managed items have a line-item number. Examples of this type of equipment are—

- Single-channel ground and airborne radio system.
- Joint Network Node.
- Command Post Node.
- Satellite Transportable Terminal.
- SMART-T.
- TRILOS.
- Scalable Network Node.
- TROPO.
- Transportable Terrestrial Command Communications.
- Phoenix.

NON-STANDARD EQUIPMENT

5-7. Non-standard equipment does not go through the formal life cycle management process because of an urgent need to support the unit's mission. Units acquire non-standard equipment to meet immediate operational needs through rapid fielding initiatives and urgent operational needs statements. Non-standard equipment includes commercial off-the-shelf equipment such as—

- Network access points.
- Satellite telephones.
- Broadband global area network.
- Proliferated low Earth orbit SATCOM.

TWO-LEVEL MAINTENANCE

5-8. The Army uses a two-level maintenance system. The two levels of maintenance are field maintenance and sustainment maintenance.

5-9. The goal of the maintenance system is to reduce repair times by repairing or replacing components, modules, or assemblies as close to the point of use as possible. Commanders, staffs, maintainers, and planners must understand two-level maintenance fundamentals to plan and execute their mission.

FIELD MAINTENANCE

5-10. Field maintenance takes place at or near the point of use. Equipment operators, operator-maintainers, and ordnance-trained maintainers perform field maintenance on or near the system. The owning unit retains the equipment or receives it back from the maintenance support facility when repairs are completed. Army maintenance units also provide field maintenance support.

5-11. Field maintenance consists of operator and crew maintenance and maintainer maintenance. Field maintenance restores unserviceable equipment using line replaceable unit or module replacement to make repairs. The owning unit normally performs field maintenance using organic tools and test equipment. Field maintenance

is not limited to removal and replacement actions. If the operator, crew, or maintainer has the skills, special tools, repair parts, technical manuals, and time to repair an item, the unit should not evacuate equipment for sustainment maintenance.

5-12. Remark codes in the maintenance allocation chart explain each task, whether operator or maintainer. The maintenance allocation chart may indicate whether to evacuate an end item or service it on-site. If operators exhaust their troubleshooting and repair capabilities, they should request on-site support or equipment evacuation from the communications-electronics maintenance shop. The maintenance facility coordinates with the S-3 for external technical support from CECOM logistics assistance representatives or field service representatives.

5-13. Field maintenance performed by operators, crew members and maintainers includes—

- Adjustment.
- Alignment.
- Service.
- Field-level modification work orders.
- Fault or failure diagnosis.
- Battle damage assessment and repair.
- Recovery.

5-14. Field maintenance entails repair and return to the user. Maintainers at echelons below brigade reside in the owning unit, forward support company, and field maintenance company.

Operator and Crew Maintenance

5-15. Signal operators inspect, service, lubricate, adjust, and replace parts and subassemblies according to the maintenance allocation chart in the system technical manual. Operators and crews are typically the first to observe equipment faults or failures. In many instances, operators or crews can repair the fault or mitigate its impact to accomplish the mission. Operators and crews may also initiate maintenance tasks in response to faults, failure indicators, or failed diagnostic tests. Operator and crew tasks in the maintenance allocation chart reference the appropriate technical manual for basic troubleshooting, removal, and replacement procedures.

5-16. Operators and crews are specialists on their systems with formal or functional training on diagnosing system faults. Operators and crews troubleshoot their systems using the appropriate technical manual and simplified or embedded diagnostic equipment to identify, isolate, and trace problems. If operators and crews exhaust their maintenance capabilities, the unit contacts the forward support company for maintenance support.

5-17. Operator-maintainers working with communications systems and communications-electronics equipment will follow the tiered approach to diagnosing system faults. The tiered approach includes—

- 1st line of support: team leader.
- 2nd line of support: squad leader.
- 3rd line of support: platoon sergeant.

- 4th line of support: network management technician.
- 5th line of support: communications-electronics maintenance shop.
- 6th line of support: field service representative.
- 7th line of support: CECOM.
- 8th line of support: project manager.

Note. Unit SOPs should be followed for notification of 4th, 5th, 6th, and 7th lines of support. Field service representatives and the project manager generally should not be notified until the prior lines of support are exhausted.

5-18. Commanders should ensure that all signal systems maintenance is annotated on DA Form 5988-E (*Equipment Maintenance and Inspection Worksheet [EGA]*), entered in the Global Combat Support System-Army, and being tracked by the next higher command.

Maintainer Maintenance

5-19. Ordnance Soldiers perform maintainer maintenance. Maintainers repair a component, accessory, assembly, subassembly, plug-in unit, shop replaceable unit, line replaceable unit, or other portion of the equipment, either on the system or after removal.

5-20. Depending on the system, the definition of a line replaceable unit or shop replaceable unit changes. The characterization of line or shop replaceable units for communications systems shifts as the level of troubleshooting increases in complexity.

SUSTAINMENT MAINTENANCE

5-21. Since field maintenance is closer to the point of use, it is the preferred method of repair. However, operators, crews, and unit maintenance personal sometimes lack the skills, special tools, repair parts, or authorization to complete repairs listed in the maintenance allocation chart. This may require evacuating equipment for sustainment maintenance. Based on the damage or failure, leaders determine the best course of action, considering the operational and mission variables.

5-22. Sustainment maintenance restores equipment to a national standard; after restoration, the equipment returns to the supply system. Sustainment maintenance requires evacuating the equipment to a support facility. When a unit sends equipment to a sustainment maintenance organization, the unit removes the equipment from its property book. Only in rare instances, such as unit reset, does the equipment return to the unit. The organic communications-electronics maintenance facility manages equipment exchanges and warranty actions.

5-23. The intent of sustainment maintenance is to return items to a national standard, to provide a consistent and measurable level of reliability. Sustainment maintenance supports both operational forces and the Army supply system. Sustainment maintenance consists of—

- Depot-level maintenance.
- Below depot-level maintenance.

Depot Maintenance

5-24. Depot level maintenance provides depot-level sustainment maintenance for communications-electronics systems, including joint SATCOM and joint command, control, communications, computers, intelligence, surveillance, and reconnaissance systems. Besides depot repairs and spares management, depot level maintenance can provide on-site depot-level technical assistance.

5-25. Tobyhanna Army Depot's forward repair activities provide depot-level sustainment presence at locations inside and outside the continental United States. Tobyhanna Army Depot's field service representatives provide depot-level technical assistance visits for on-site troubleshooting, repair, and configuration assistance worldwide.

Below Depot Maintenance

5-26. The CECOM Field Sustainment Support Division has seven regional support centers aligned with the Army field support brigades. Regional support centers provide forward logistical support, including care of supplies in storage, warehousing, below depot sustainment maintenance, and return maintenance authorizations for warranty items. The regional support centers can react rapidly to unit requirements and support surge requirements, if necessary. Regional support centers mainly support commercial off-the-shelf and non-standard equipment.

5-27. CECOM provides below depot sustainment maintenance for United States Army Training and Doctrine Command training base tactical equipment at Fort Huachuca, Arizona and Fort Gordon, Georgia. This includes associated support items of equipment for the systems.

5-28. CECOM's logistics assistance representatives provide commanders the technical guidance necessary to resolve problems with weapon systems, equipment, and logistics. Logistics assistance representatives help solve readiness issues at unit level, and assist with logistics problems beyond the unit's resources or capabilities to resolve through—

- Technical guidance to resolve equipment and systemic logistics issues.
- Analysis of readiness issues.
- Identification of systemic issues with command, control, communications, computers, and intelligence equipment.

Maintenance Support for Tactical Signal Battalions in Theater

5-29. Companies, platoons, sections, and teams that deploy separately receive communications electronics maintenance support from the supported unit. Deployed communications support packages under operational control of units in support of theater operations receive field-level maintenance support from the local organization. If the supported organization is unable to provide maintenance services and repairs for unit-unique equipment, the mission may require the deployment of the communications support package's organic maintenance assets to fulfill the maintenance requirement. The communications electronics maintenance section performs all maintenance tasks for communications and signal systems and assemblages within the expeditionary signal battalion and provides routine, scheduled, and emergency maintenance support and

spares management on unique command and control systems and signal communications platforms.

5-30. The designated theater signal brigade and corps signal brigade coordinate the maintenance and logistics support of their deploying communications support package in advance. During maintenance planning, consideration for funding, locations (the continental United States or outside the continental United States), and supported communications assemblages for deployment are critical.

Non-Organic Sustainment Maintenance Requests

5-31. Communications support packages request sustainment-level maintenance support when maintenance services are beyond the scope of field-level maintenance, as described in the maintenance allocation chart. A communications support package may also require sustainment-level maintenance if tools and test equipment are not available or if proprietary testing is required.

5-32. The communications support package's maintenance personnel coordinate sustainment-level communications-electronics maintenance with the field support brigade. The field support brigade does not perform sustainment-level maintenance organically; instead, the theater Army field support brigade coordinates with the nearest logistics assistance representative that either uses field service representatives to conduct sustainment-level maintenance; exchange the faulty equipment with a serviceable replacement; or evacuate the equipment to the nearest depot.

Non-Organic Sustainment-Level Motor and Generator Maintenance

5-33. Communications support packages include tactical vehicles for maneuvering personnel, communications systems, and ancillary equipment. Additionally, communications support packages have tactical generators for supplying electrical power to communications systems. Communications support packages may require sustainment-level maintenance in the theater and will use an area maintenance and supply facility. The communications support package coordinates for assistance from the area maintenance and supply facility through the field support brigade. Table 5-1 on page 95 shows the alignment of units to type of maintenance performed.

Table 5-1. Alignment of units to type of maintenance performed

Field Maintenance	*Sustainment Maintenance*
Operator and crew	Regional Support Center
Forward support company	Specialized Repair Activity
Field maintenance company	Forward Repair Activity
Support maintenance company	United States Army Materiel Command support formation
Other units with assigned ordnance-trained maintainers	Army depots—Tobyhanna, Anniston, Letterkenny
Army field support brigade (management only)	
Army field support battalion	
Logistics readiness center (installation)	

COMMUNICATIONS-ELECTRONICS MAINTENANCE

5-34. The unique maintenance requirements of signal equipment and the need to maintain the DODIN-A with minimal downtime requires rapid maintenance response. Some operator-maintainers can perform more extensive field maintenance on their assigned equipment at the point of use. These operator-maintainers perform equipment replacement tasks to restore or maintain the DODIN-A.

NETWORK MAINTENANCE

5-35. Maintaining the DODIN-A requires continual coordination between signal leaders and staffs. Signal staffs collaborate across organizational boundaries to sustain their portions of the DODIN-A. Units must be capable of employing and maintaining their communications equipment and leveraging the technical expertise and knowledge of logistics assistance representatives and field service representatives as a part of their maintenance strategy.

5-36. The network management technician and the electronic systems maintenance warrant officer handle requests for external support of command and control information systems, tactical network systems, and tactical radios. This ensures centralized reporting and readiness efforts from CECOM, the brigade logistics support team, the regional support center, and contract field service representatives.

SPARES MANAGEMENT AND ACCOUNTABILITY

5-37. The organic communications-electronics maintenance element performs spares management for command and control information systems, network systems, and other signal platforms, except for on-board spares designated as components of an end item. Central management of signal spares by the organic maintenance element expedites replacement of unserviceable items, enables fault verification, generates requisition demand history, and pools limited spares so they are available across the command. If spares management is decentralized, the relatively lower local demand may not support retention of the spares as shop stock or authorized stockage list items.

5-38. Spares management affects various quarterly, semi-annual, and annual services on major signal platforms. Communications-electronics technicians verify faults to avoid unneeded evacuation of spares without confirmed hardware, software, or firmware faults. Evacuation of items with no evidence of fault wastes operational funds and reduces the pool of available spares. Global Combat Support System-Army can generate a supply demand history for spares, even if they are replaced under warranty or through standard requisition processes. The collection of demand history aids analysis of maintenance trends, helps identify systemic parts failures, and records line replaceable unit demand to inform procurement actions by the item manager.

5-39. Communications-electronics maintenance facilities can better manage spares and provide the flexibility to support various mission requirements at the company or team level. The S-3 collaborates with the electronic systems maintenance officer to tailor a logistics package to support training and operational missions. This allows for maintenance prioritization, balanced use of support, and efficient use of spares.

Physical Security of Spares

5-40. Physical security of signal spares remains an accountability concern, based on historical trends from the loss of program manager-issued spares. Maintenance plans must address securing, organizing, and protecting signal spares from in-transit damage. Table of organization and equipment-authorized storage containers may not be sufficient. With the steady influx of spares for all other systems, a formation's organic storage capacity is even more strained.

Mobility of Spares Storage

5-41. Units may require multiple lifts or be forced to prioritize movement of multiple spares containers. Lesson learned indicate commanders should consider procurement of additional Army-approved storage solutions to increase capacity. Portable, customizable containers or hardened transit cases with foam inserts are common storage options to mitigate capacity and mobility shortfalls.

Environmental and Weather Impacts Affecting Spares

5-42. Fully or partially environmentally controlled storage areas are essential in areas prone to extreme heat, humidity, and moisture. High-cost, low-density electronic and electrical components may fail after long exposure to harsh environments. Most signal equipment spares are sensitive to environmentally induced failures due to corrosion or electrostatic discharge. Without deliberate measures to mitigate these conditions, spares may not be functional or available when needed. Commanders get increased operations and maintenance funding costs to replace environmentally damaged spares never used.

SECTION II – SUPPLY

5-43. Signal companies may need to resupply deployed teams where the supported unit does not have organic spares to provide the team. In these cases, the supported unit G-4 or S-4 is responsible for coordinating movement for the spares. The supported unit G-4

or S-4 will coordinate with other units in the assigned area to request equipment spares. See table 5-2 for an overview of the classes of supply.

Table 5-2. Classes of supply

Class	*Description*
Class I	Subsistence, including health and welfare items.
Class II	Clothing, individual equipment, tentage, tool sets and tool kits, hand tools, administrative, and housekeeping supplies and equipment (including maps). This includes items of equipment, other than major items, prescribed in authorization/allowance tables and items of supply (not including repair parts).
Class III	Petroleum, oils, and lubricants: petroleum and solid fuels, including bulk and packaged fuels, lubricating oils and lubricants, petroleum specialty products; solid fuels, coal, and related products.
Class IV	Construction materials, to include installed equipment and all fortification/barrier materials.
Class V	Ammunition of all types (including chemical, radiological, and special weapons), bombs, explosives, mines, fuses, detonators, pyrotechnics, missiles, rockets, propellants, and other associated items.
Class VI	Personal demand items.
Class VII	Major items: A final combination of end products which is ready for its intended use: (principal item) for example, launchers, tanks, mobile machine shops, vehicles.
Class VIII	Medical materiel, including medical peculiar repair parts.
Class IX	Repair parts and components for equipment maintenance.
Class X	Nonstandard items to support nonmilitary programs such as agriculture and economic development.

RESUPPLY

5-44. The commander can also leverage military airlift for resupply; however, military airlift may not be as agile as a private company. The commander will need to decide based on the circumstances on the ground on how best to get teams the equipment needed in these special circumstances.

5-45. Resupply operations are either planned or emergency. Examples of planned resupply to maintain routine resupply operations include—

- Logistics package.
- Caches.
- Modular system exchange (flatrack exchange).
- Pre-positioned supplies.

5-46. The company SOP should specify cues and procedures for each resupply method. The company rehearses resupply operations during company training exercises. The actual method selected for resupply in the field depends on mission variables.

ROUTINE

5-47. A logistics package is a simple and efficient method to accomplish routine resupply operations. These operations include regular resupply of items in classes I, III, V, and IX and of any other items requested by the company. Planning for a logistics package takes place at battalion level and normally occurs at every opportunity. The logistics package consists of company and forward support company assets that transport supplies to the company.

5-48. The company supply sergeant, battalion S-4, and the forward support company assemble the logistics package in the battalion field trains area under the supervision of the designated personnel, typically a representative from the battalion S-4.

5-49. Once the logistics package is prepared for movement, the supply sergeant accompanies the vehicles forward from the field trains command post and convoys to either the combat trains command post or to the logistics release point. The first sergeant, platoon sergeant, or other representative meets the logistics package and guides it to the company resupply point. The company replenishes each platoon; the platoons, in turn, disperse supplies to each section or team.

5-50. The tactical situation dictates which technique of resupply the company uses: tailgate, service station, a variation of one type, or a combination of both types. The situation also dictates when to resupply. Generally, the company should attempt to avoid resupply during offensive operations. Resupply should take place during mission transition whenever possible. Resupply is unavoidable during long duration defensive missions.

Tailgate Resupply

5-51. In the tailgate resupply technique, the first sergeant, platoon sergeant, or other designated person will bring the logistics package to individual section locations. This method is used when routes leading to vehicle positions are available, terrain permits movement of multiple vehicles to each platoon position and the unit is not under direct enemy observation and fire. Signal sections can remain in established positions to allow vehicles carrying class I, class III, and class V supplies to reach them.

5-52. Individuals can rotate through the feeding area, pick up mail, and fill or exchange water cans. Tailgate resupply is time-consuming, but it is useful in maintaining stealth during defensive missions, because combat net radio and at-the-halt assemblages do not have to be broken down to move. If necessary, supplies can be hand carried to section or team positions to further minimize signatures. Figure 5-1 on page 99 shows an example of a tailgate resupply operation.

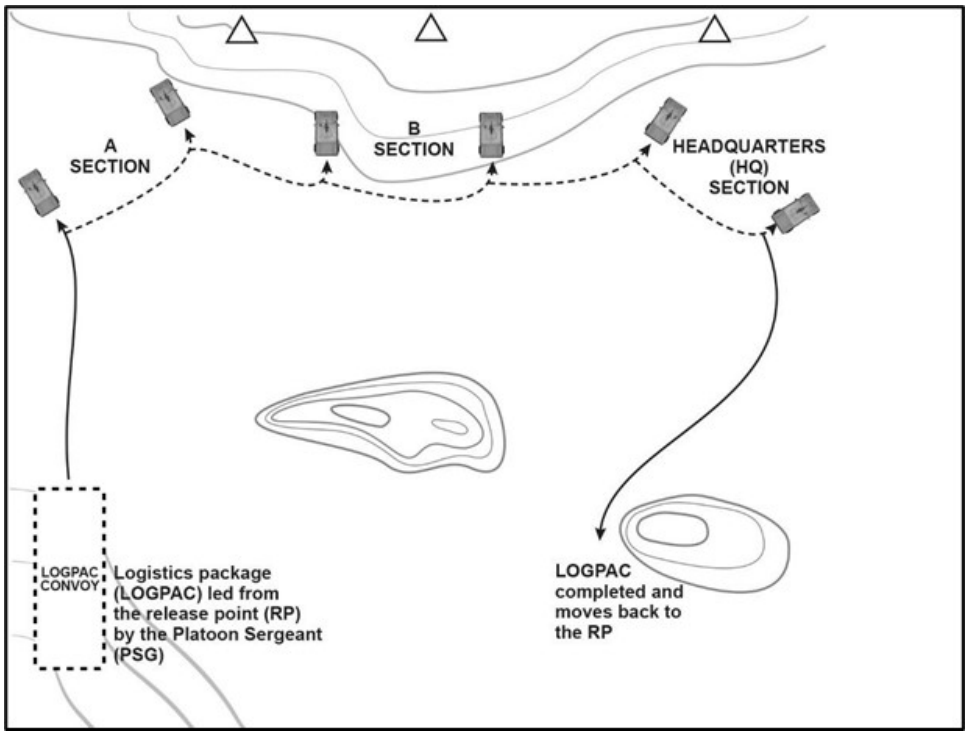


Figure 5-1. Tailgate resupply

Service Station Resupply

5-53. In the service station resupply technique, vehicles or individuals move to a designated location to rearm, refuel, and resupply, or turn in damaged equipment. The platoon leader directs the platoon sergeant to rotate vehicles or sections through the resupply site based on the enemy situation and shortages in the platoon. This process continues until the entire platoon has been replenished.

5-54. When using service station resupply, the vehicles and individuals enter the resupply point following one-way traffic flow and only vehicles requiring maintenance stop at the maintenance holding area. The maintenance element can help the operator or crew in verifying preventive maintenance checks and services of their vehicles. Maintainers can correct minor deficiencies on the spot with available tools, repair parts, and battle damage assessment and repair techniques.

5-55. Each vehicle or individual rotates through the supply location, with teams rotating through to eat, pick up mail, and refill or exchange water cans. Service station resupply is inherently faster than the tailgate method because vehicles must move and concentrate, however, it can create security problems and disrupt signal support. During defensive missions, the platoon leader must create a plan to rotate the platoon based on shortages and must be careful not to compromise the location of assemblages or disrupt service. Figure 5-2 on page 100 is an example of a service station resupply operation.

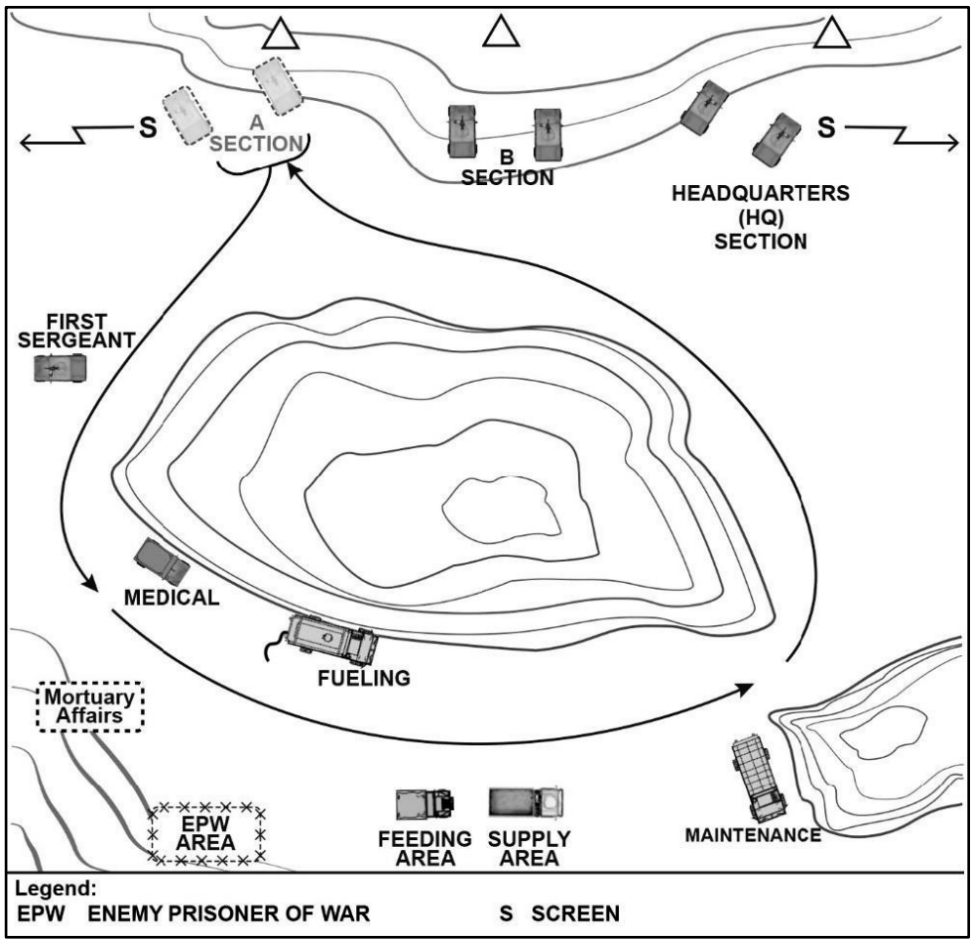


Figure 5-2. Service station resupply

EMERGENCY

5-56. Emergency, or immediate, resupply normally involves class III and class V supplies, and takes place when the platoon has such an urgent need for resupply that it cannot wait for the routine logistics package. Retransmission teams not co-located with a larger organic element will likely need emergency resupply at some point.

5-57. Once requested through the commander or executive officer, an emergency resupply can be conducted using either the service station or tailgate technique. The unit usually uses the quickest appropriate means between the two techniques:

Tailgate Technique

5-58. In the tailgate technique, limited supplies are brought forward to the closest concealed position. Individual vehicles or sections disengage and move to a resupply

point, obtain their supplies, and return to their assemblage or to continue or reestablish service. This is a version of the service station technique.

Service Station Technique

5-59. In the service station technique, individual vehicles or sections disengage and move to a resupply point, obtain their supplies, and return to their assemblage or to continue or re-establish service.

PRE-POSITIONED RESUPPLY OR CACHE

5-60. As with all operations, leaders consider the mission variables of METT-TC (I) and sometimes need pre-positioned or cached supplies. During a movement to contact or offensive operations, signal teams will likely cache supplies not needed during the operation. The caching unit or another friendly unit requiring those cached supplies will retrieve the supplies later. Appropriate materials for caching for a signal team are supply classes I, III, and V. Units should not cache sensitive items or on-hand spares.

This page intentionally left blank.

Chapter 6
Unit Training

Proper command emphasis can ensure operators and teams are proficient on their systems before field exercises. This training may take place in the unit's motor pool or a garrison training area, with or without the need for satellite time. Units frequently only make time for operator training when the unit goes to the field. This is not an acceptable practice, since network disruptions interfere with the larger exercise.

SECTION I – TRAINING IN THE COMPANY

6-1. At the company level, training models are developed and used as a simple and effective planning and execution tool for small-unit and individual training events. Training models are a general framework of the major activities and steps to plan training; they do not provide enough detail to develop the unit training plan or to develop and coordinate training events. The unit can modify training models based on time and resources available.

6-2. Signal training should be a deliberate, sequential, and progressive process embedded in the unit training plan. Commanders need to understand the importance of providing enough time and resources for signal training. If commanders and staffs do not provide sufficient training time or exercise their organic capabilities with rigorous, realistic training, they put the overall unit training plan and mission at risk.

6-3. Signal training is predicated on properly maintained equipment. Consequently, communications-electronics maintenance must be integral to signal training. Commanders should deliberately plan and execute maintenance on a regular basis. Signal training and maintenance is coordinated at all levels over the planning horizon to support unit readiness. For further discussion of communications-electronics maintenance guidelines, see chapter 5.

6-4. The foundation of signal support is an organization of competent, confident, and cohesive crews and sections. Commanders should emphasize training to build crews and sections that can employ signal systems and nodes, operate independently, and build capability over time. Commanders use the 8-step training model (see paragraph 6-20) to verify they have executed the major steps to plan and resource signal training.

COLLECTIVE TRAINING TECHNIQUES

6-5. Collective training follows an integrated approach of live, virtual, and constructive training at home station, combat training center rotations, and during deployments to build confident, cohesive units able to adapt to their environment and defeat the enemy. Demanding and repetitive training builds Soldiers' confidence in their weapons and equipment, their leaders, their teams, and their ability to fight and overcome challenges.

REALISTIC TRAINING ENVIRONMENT

6-6. The training environment should duplicate the anticipated operational environment and threat. Teams train under conditions that emphasize change, uncertainty, degraded friendly capabilities, capable enemies, and austere conditions. Realistic training prepares Soldiers to perform under combat conditions by including unexpected tasks and battle drills.

6-7. Commanders should incorporate a realistic threat environment into training exercises, so teams learn to recognize indications of malicious cyberspace activities and electromagnetic interference. Understanding network vulnerabilities is critical. The training environment should include likely adversary tactics, techniques, and procedures. Establishing a properly configured, monitored, and secured network during training events prepares operators to detect malicious and unauthorized activity and enables command and control and the other warfighting functions.

Note. Units should create a training environment that reflects the anticipated operational environment as much as possible. Commanders can use TC 7-100.2 to build realistic training environments.

6-8. Integrating training with a realistic threat able to attack networks into unit training at home station and combat training centers prepares units for real-world missions. It also prepares units to understand the threat and indicators of a contested environment. Realistic training also demonstrates the consequences of not following security procedures.

6-9. A realistic training environment provides operators practice securing the network against active threat and allows units to integrate actions and effects. Training signal forces to secure the network against an active threat is critical to mission success. Realistic, combat-focused training requires specialized technical training, instrumentation, and ranges at home station and combat training centers.

DIGITAL BATTLE DRILLS

6-10. Unit SOPs should establish digital battle drills for a range of likely emergencies. Digital battle drills provide operators structured, pre-planned responses to network, COMSEC, cybersecurity, or server-related events or power outages. Realistic training and repetition ensure operators can perform conditioned responses reflexively under combat or other emergency conditions.

COMBINED ARMS TRAINING STRATEGY

6-11. The signal company’s training calendar should include events from the combined arms training strategy. These training events progressively build from team level through multi-echelon exercises supporting the parent unit. The combined arms training strategy begins with team tasks to develop crew proficiency installing and operating assigned systems. Successive platoon- and company-level training exercises ensure the teams can integrate network systems into the DODIN-A. Training signal teams to proficiency through the combined arms training strategy ensures Soldiers remain

proficient in their individual military occupational specialty skills and can integrate the network to support operations.

6-12. The combined arms training strategy database is built into the Army Training Network Website. The database is searchable from the search box along with training and evaluation outlines and unit mission-essential task lists. This combination of tools should be used to understand and conduct the training and evaluation outlines and battle drills.

6-13. Combined arms training strategies are templates to build a unit training plan based on a unit's designed mission, functions, and capabilities. Combined arms training strategies use task sets-groups of tasks logically trained together during training events using the crawl-walk-run methodology. Combined arms training strategies reference and recommend who, what, how, and how often to train a task to reach task proficiency. They recommend resources, prerequisites and provide purpose, outcome, and execution guidance.

6-14. Combined arms training strategies organize the unit task list to train and enable the unit to provide the commander with the capabilities the unit is designed to provide. The company's training strategy should include reacting to and conducting tasks under chemical, biological, radioactive, and nuclear conditions with mission oriented protective posture.

6-15. Leaders from the commander down to the team leader should be familiar with the Army Training Network and combined arms training strategy database. Team leaders should download and print training and evaluation outlines for their team.

TRAINING AND EVALUATION OUTLINES

6-16. Training and evaluation outlines and drills are training aids available as templates that can be modified to meet specific unit needs. Training and evaluation outlines and drills are located on the Army Training Network and Central Army Registry Websites. Commanders can add and remove tasks or steps to meet their readiness requirements. The combined arms training strategy tool guides the unit training process as outlined in FM 7-0.

6-17. Leaders can download the appropriate training and evaluation outline for each specific task. Training should be planned well in advance and the team should have already completed table I of the signal assessment tables.

6-18. A training and evaluation outline describes the task, conditions, and standards for training and is the Army standard for training and evaluating individual and collective tasks. Performance task steps and performance measures are evaluated using a go or no-go basis.

6-19. All training should be graded to standard by an officer or noncommissioned officer based on echelon using the training and evaluation outline. Training requirements are met when—

- The task or event is conducted within a properly configured single threat training environment at night.
- 75% or more of leaders are present with more than 80% of Soldiers present.

- The evaluated element receives a go on 80% or more of the performance measures-all critical performance measures at least 85% go on leader performance measures.
- The capstone event is conducted during an external evaluation.

8-STEP TRAINING MODEL

6-20. One common model to plan training events at company-level and below is the 8-step training model (see figure 6-1). The 8-step training model is a flexible framework to plan and manage simple training events.

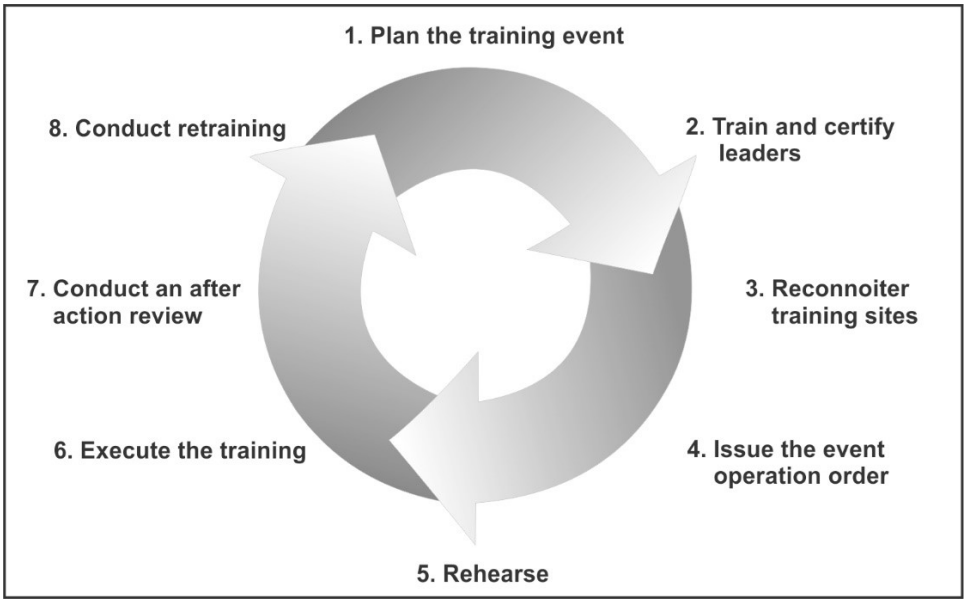


Figure 6-1. The 8-step training model

STEP 1 – PLAN THE TRAINING EVENT

6-21. During step 1, company leaders develop specific, attainable, and measurable training objectives based on the commander's training guidance. Leaders should allocate and schedule enough time for the event on the company training schedule. During planning, leaders—

- Design and establish the operational environment to support the evaluated training objectives. Refer to TC 7-102 for establishing an operational environment during training.
- Identify resources needed, including training areas, simulators, supplies, and outside trainers.
- Identify potential training hazards and mitigate associated risks. Refer to ATP 5-19 for more information about risk management.
- Develop training support and assessment plans as the basis for demanding, realistic training.

6-22. Leaders should use the combined arms training strategy to assist in planning unit training. The combined arms training strategy provides resources needed to plan and conduct unit training. Some of the resources include—

- Mission-essential task lists.
- Unit task lists.
- Training events matrix.
- Collective tasks.
- Event list.

6-23. Leaders can also use the Army Training Network Website to assist with more training tools. Other resources on the Army Training Network are—

- Digital Training Management System.
- Training and evaluation outlines.
- Small unit leader tool.

STEP 2 – TRAIN AND CERTIFY LEADERS

6-24. Step 2 involves training and certifying leaders, including officers, noncommissioned officers, civilians, and qualified individual Soldiers. The certified leaders then train and certify other leaders. Qualified personnel demonstrate their subject matter expertise and proficiency in performing the training task or tasks to the objective standard. The train-the-trainer concept ensures leaders and trainers can effectively instruct and certify the unit. Step 2 also includes training and certifying opposing force elements and training role players to create a realistic, threat-based training environment.

6-25. Signal teams gain certification using training and evaluation outlines for individual and collective tasks. Certifications should be maintained by the training noncommissioned officer annually. Certifying leaders must be certified in the training they are evaluating.

STEP 3 – RECONNOITER TRAINING SITES

6-26. Leaders conduct a reconnaissance of proposed training areas and facilities. The leaders' reconnaissance verifies the location can support the proposed training and allow the unit to achieve its training objectives.

6-27. During step 3, leaders verify all necessary resources, training areas, and training support plans are properly coordinated, scheduled, and prepared for the training event. Leaders contact support site personnel and review scheduling and coordination issues. If necessary, leaders modify the training plan to meet site requirements and maximize training opportunities.

STEP 4 – ISSUE THE EVENT OPERATION ORDER

6-28. The event OPORD ensures subordinates have the information needed to execute the training event. Through the OPORD, the commander clearly identifies the tasks to be trained, the training objectives, and a clearly understandable mission statement. The OPORD communicates the scope of the training, how to conduct the event, and the tasks to train and evaluate. Successful training events require all leaders to understand the expected training outcome, based on the commander's intent and objectives.

STEP 5 – REHEARSE

6-29. Rehearsals are critical to the execution of any operation or training plan. All personnel involved in the training event participate in rehearsals to ensure they understand and can synchronize and prepare for their roles. Company leaders supervise training rehearsals to ensure the company is prepared to conduct organized and effective performance-oriented training. This step also includes conducting opposing force rehearsals.

STEP 6 – EXECUTE THE TRAINING

6-30. Commanders ensure the training event occurs as planned and scheduled. Effective training events require—

- Maximum participation of the training audience and leaders.
- Minimum training distractors.
- Leader involvement to check and supervise training, where necessary.

6-31. The designated trainers train Soldiers to ensure they can meet the training objective. While unplanned contingencies often arise, commanders and platoon leaders should make every effort to avoid cancelling a planned training event.

6-32. Training should prioritize the use of effective training variables to ensure a trained status. Within the task, condition, and standard framework for training, creating appropriate operational environment conditions is a critical criterion for training and unit readiness reporting. These operational environment conditions are one of several criteria for achieving task proficiency ratings of trained, practiced, or untrained. Trainers and exercise planners must understand the construct and influence of the operational variables and relevance to the mission variables of METT-TC (I). Figure 6-2 on page 109 shows an example of a training variable assessment table.

Plan and Prepare			Execute						Evaluate	
Operational Environment SQD & PLT		Training Environment (L/V/C)	% Leaders present at training/authorized	% Present at training/authorized	External evaluation	Performance measures	Critical performance measures	Leader performance measures	Evaluator's observed task proficiency rating	Commander's assessment
Dynamic (Signal Threat)	Night	At the discretion of the Commander IAW unit Combined Arms Training Strategy (CATS), External Evaluations (EXEVAL) must be conducted in a live environment	>=75%	>=80%	Yes	>=80% GO	All	>=85% GO	T	T
Static (Single Threat)	Day		60-74%	60-79%	No	65-79% Go	<All	75-84% GO	P	P
			<=59%	<=59%		<65% GO		<=74% GO	U	U

209 **Figure 6-2. Training variable assessment table**

210 ## STEP 7 – CONDUCT AN AFTER ACTION REVIEW

211 6-33. During and after training, leaders—
212 • Review the tasks trained.
213 • Assess the unit's training level compared to the training objective.
214 • Collect lessons learned to improve future training events and tactics,
215 techniques, and procedures.

216 6-34. Commanders should facilitate in-depth after action reviews, staying away from
217 the common three ups and three downs. Facilitated after action reviews are in depth
218 discussions of who did what, why they did it, and how they could have done it better.

219 6-35. Facilitated after action reviews start a cognitive thought process in which all
220 parties are involved in the discussion. Commanders record these assessments in the
221 Digital Training Management System for use in future training events or inclusion in
222 the unit SOP.

STEP 8 – CONDUCT RETRAINING

6-36. Units should not end a training event until all scheduled tasks are trained to standard and all training objectives are met. Leaders and trainers should retrain tasks until the training audience achieves the standard before concluding the event.

6-37. Units often neglect retraining due to time or resource limitations or conflicting scheduling requirements. However, retraining is often the most critical step. Training to established standards builds competence and instills confidence in units, leaders, and Soldiers. Commanders and subordinate leaders must honestly and objectively assess their unit's ability to meet performance standards. Refer to FM 7-0 for more information about unit collective training and the 8-step training model.

SAFETY

6-38. In a training environment, leaders must perform a risk assessment before each training event in accordance with ATP 5-19. Leaders complete the DD Form 2977 (*Deliberate Risk Assessment Worksheet*) during the planning and completion of each task and sub-task by assessing the risk factors and the mission variables of METT-TC (I).

ELECTROMAGNETIC RADIATION HAZARDS

6-39. Radiation hazards for signal units will most often be microwave radiation emitted from equipment. Transmission equipment including TROPO, line of sight and SATCOM all emit microwave radiation which can cause headaches and soreness in Soldiers and possibly kill vegetation in the direct path of the transmission beam.

6-40. Safe range measurements are specified in the equipment technical manual. These safe distances vary based on equipment. For instance, for a Satellite Transportable Terminal with Ku band feed installed, the minimum safe distance is 110 meters in the main radiating beam of the antenna when the system is transmitting. For the Satellite Transportable Terminal with the Ka band feed installed, the minimum safe distance is 166 meters in the main radiating beam of the antenna when the system is transmitting.

6-41. Leaders should ensure Soldiers follow safe distances specified in the technical manuals and safety concerns are being met. Soldiers should block the area off with engineer tape and a radio frequency warning placard.

HEAVY LIFTING

6-42. Equipment used by expeditionary signal companies may require a two-man lift or higher. Equipment technical manuals specify how many Soldiers should be moving each piece of equipment. Transport cases often state the equipment's recommended carrying capacity, however, this precaution can fade over time. Leaders should ensure the right number of Soldiers lift the equipment and Soldiers apply proper lifting techniques, such as lifting the equipment with the knees and not the lower back.

CONVOY OPERATIONS

6-43. Signal units perform convoy operations to enable communications throughout the operational environment, providing the maneuver commander with flexibility and operational reach. This helps to optimize coordination and communication between

vehicles and personnel, and to ensure that the convoy can operate efficiently and safely. Leaders must also consider convoy security, towing equipment, uneven terrain, and limited visibility to ensure the safety of convoys. See paragraph 3-95 for more information about military aspects of terrain. For more information on towing hazards and concerns, refer to TC 21-305-1.

Convoy Security

6-44. The responsibility of ensuring the safety and protection of a convoy is with the convoy commander, who may delegate the responsibility to another leader. The commander has the duty to maintain the correct ratio of security vehicles or gun trucks to other vehicles in the convoy, based on local or theater requirements and standard operating procedures. The team should conduct rehearsals of battle drills for the most likely and most dangerous enemy courses of action before embarking on the mission, and these drills should be discussed during the convoy brief. Refer to ATP 4-11 for more information about convoy operations.

Limited Visibility

6-45. Conditions that limit visibility can be classified into two categories - natural and man-made. Natural conditions comprise of situations such as night-time, fog, rain, snow, smoke, and sandstorms. Man-made conditions include transparent armor or ballistic glass, blind spots occupied by equipment placed in the vehicle, as well as urban obstacles such as buildings, overpasses, and narrow streets lined with parked vehicles. These conditions can pose a significant threat to safety during convoy operations and must be carefully considered and managed.

Electrical Shock

6-46. The power generation equipment used in expeditionary signal companies presents a risk of electrical shock. Leaders should ensure Soldiers use personal protective equipment while working with equipment. Other practices to help mitigate electrical hazards are—

- Know where the hazards are.
- Properly maintain equipment.
- Do not expose parts or energized surfaces.
- Inspect cabling prior to use.
- Remove jewelry and identification tags.
- Ensure power cables have a drip loop to prevent damage.

6-47. All powered equipment should be properly grounded. Refer to TC 6-02.6 for more information about grounding communications systems.

Fueling and Refueling Hazards

6-48. Fueling and refueling presents the risk of spillage, fire, and explosion if handled improperly. Soldiers should practice safe fuel handling and refueling operations to mitigate spillage and fire hazards. For more information on fuel supply operations refer to ATP 4-43.

TRIP HAZARDS

6-49. Soldiers operating in a field environment mitigate trip hazards by properly running data cables along edges of buildings or bundling them neatly. Ground rods should be properly installed and parallel with the hole around them. Ground straps should be flush with flat surfaces and not pulled tight lifting above the ground. Antenna guy wires should be properly installed and marked with engineer tape and or chemical lights, depending on the mission and environment.

HEAT CASUALTIES

6-50. High levels of physical activity in high temperatures can lead to heat injuries. Leaders should plan work-rest cycles and monitor Soldiers' water consumption during training and operations. See table 6-1 for the work-rest cycle and water consumption table. The two different types of heat casualties are heat exhaustion and exertional heat stroke.

Table 6-1. Work-rest cycles and water consumption

Heat category	*WBGT [1,2] index degrees F*	*Easy work*		*Moderate work*		*Hard work*	
		Work/ rest [3,4]	*Water intake [5] qt/hr*	*Work/ rest min*	*Water intake qt/hr*	*Work/ rest min*	*Water intake qt/hr*
1 (WHITE)	78 to 81.9	NL[6]	0.50	NL	0.75	40/20	0.75
2 (GREEN)	82 to 84.9	NL	0.50	50/10	0.75	30/30	1.00
3 (YELLOW)	85 to 87.9	NL	0.75	40/20	0.75	30/30	1.00
4 (RED)	88 to 89.9	NL	0.75	30/30	0.75	20/40	1.00
5 (BLACK)	More than 90	50/10	1.00	20/40	1.00	10/50	1.00

[1]If wearing body armor, add 5° F to WBGT index in humid climates.
[2]If wearing IPE (MOPP 4), add 10° F to WBGT index for easy work, and 20° F to WBGT index for moderate and hard work.
[3]The work/rest times and fluid replacement volumes will sustain performance and hydration for at least 4 hours of work in the specified heat category. Fluid needs can vary based on individual difference (± 0.25 qt/hr) and exposure to full sun or full shade (± 0.25 qt/hr).
[4]Rest means minimal physical activity (sitting/standing), accomplished in shade if possible.
[5]CAUTION: Hourly fluid intake should exceed 1.5 quarts and daily fluid intakes should not exceed 12 quarts.
[6]NL = No limit to work time per hour (hr).

LEGEND:

F	**Fahrenheit**	**NL**	**no limit**
hr	**hour**	**qt**	**quarts**
min	**minute**	**WBGT**	**wet bulb globe temperature**
MOPP	**mission-oriented protective posture**		

Heat Exhaustion

6-51. Heat Exhaustion occurs when more fluid is lost from sweating and respiration than is taken in, so there is not enough fluid to cool the body off.

Signs and Symptoms

- Dizziness, headache, nausea, unsteady walk, weakness, muscle cramps, fatigue, and chills.
- Core temperature elevated but remains below 104 degrees, Fahrenheit.
- Symptoms resolve rapidly with cooling interventions.

Treatment

- Rest Soldier in shade.
- Loosen uniform and remove head gear.
- Have Soldier drink 1.5 quarts of water over 1 hour.
- Evacuate if the Soldier's symptoms show no improvement in 15–20 minutes, or if the Soldier's condition worsens.

Exertional Heat Stroke

6-52. Exertional heat stroke is caused by an increase in the body's core temperature and can lead to death. The body has plenty of fluid, but the external temperature is too high for the body to eliminate its excess heat.

Signs and Symptoms

- Persistent mental status changes, delirium, inappropriate behavior, or aggressiveness.
- Convulsions or seizures, coma, recurrent vomiting, loss of bowel control (fecal incontinence), flaccid muscles, persistent rigidity, weak or rapid pulse.

WARNING

Exertional heat strokes are a medical emergency and in severe cases can be fatal.

Treatment

- Call for emergency medical services or medical evacuation.
- Remove all outer clothing.
- Initiate rapid cooling with ice sheets.
- Cover all but the face with ice sheets.
- Ensure the ice sheet is soaked before applying to the Soldier.
- Switch ice sheets every 6 minutes with new ice sheets.

6-53. Heat casualties are armed forces reportable medical events. Leaders should verify Soldiers are documented as heat casualties once medical personnel verify their status. For more information on heat injuries refer to TB MED 507.

CAUTION

During mission oriented protective posture training, leaders must monitor personnel for potential heat injury. Local policies and procedures must be followed during times of elevated heat category to avoid heat-related injuries. Leaders consider the mission oriented protective posture work-rest cycles and water replacement guidelines in accordance with current chemical, biological, radiological, and nuclear doctrine.

SECTION II – SIGNAL ASSESSMENT TABLES

6-54. Signal assessment tables provide a tiered approach to collective signal training. The tables provide a crawl-walk-run training methodology from individual through team, section, platoon, and higher collective tasks. Signal assessment tables I–VII provide a training framework for signal training through the company level.

TABLE I – INDIVIDUAL TRAINING

6-55. During table I training, team leaders train Soldiers to conduct the individual tasks that support the team's collective tasks. Team leaders also train Soldiers on equipment maintenance during table I training. Team leaders train their teams using table I and determine when individuals are prepared for table II certification. Table I training includes personnel and equipment training.

PERSONNEL TRAINING

6-56. Military training improves the capabilities of Soldiers in their respective roles. Team leaders ensure Soldiers complete—

- Role-based cyberspace workforce training.
- Individual task training.
- Preventive maintenance training.
- AR 350-1 training requirements.

Role-Based Cyberspace Workforce Training

6-57. Cyberspace workforce training unifies the overall cyberspace workforce and establishes specific workforce elements for information technology, cybersecurity, cyberspace effects, intelligence, and enablers to align and manage the cyberspace workforce. During table I training, Soldiers complete cyberspace workforce training based on their work role. The minimum cyberspace workforce training for general-purpose users is the cybersecurity awareness challenge.

Individual Task Training

6-58. Team leaders document individual task training in the Digital Training Management System and the Soldier's individual training record. Leaders monitor Soldier training and individual task completion to certify proficiency in technical, tactical, and leadership skills. Individual task training includes common task training and military occupational specialty task training.

Common Tasks

6-59. Team leaders reinforce training in common tasks taught to Soldiers during initial entry training. Signal teams must be proficient in all common warrior tasks and battle drills. Warrior tasks and battle drills enhance a Soldier's readiness. Warrior tasks are a collection of individual Soldier skills known to be critical to a Soldier's survival. Refer to STP 21-1-SMCT for specific tasks. Examples of common tasks include—

- Weapons training.
- Tactical communications.
- Urban operations.
- First aid.

Military Occupational Specialty Tasks

6-60. Team leaders ensure Soldiers receive training specific to their military role, including the use of any specialty equipment. Soldiers perform and reinforce military occupational specialty skills during unit training events.

Preventive Maintenance

6-61. Preventive maintenance checks and services identify and correct faults and ensure continued operation of the equipment. Soldiers train to conduct preventive maintenance specified in the equipment technical manual.

AR 350-1 Training Requirements

6-62. AR 350-1 training requirements cover unit and individual training. Team leaders monitor training throughout the year and ensure Soldiers complete annual Army training requirements. Examples of AR 350-1 training include—

- Antiterrorism Level 1.
- Combatting trafficking in persons.
- Controlled unclassified information.

Equipment Training

6-63. Units conduct individual equipment training of Soldiers on their assigned equipment. Equipment training includes—

- Supply discipline.
- Operator maintenance.
- Driver training.
- Weapons training.
- COMSEC.

Supply Discipline

6-64. Team leaders enforce supply discipline by maintaining accountability of all classes of supplies. Team leaders enforce programs to ensure resources are used without fraud, waste, or abuse.

Operator Maintenance

6-65. Operators perform preventive maintenance checks and services on their assigned equipment. Based on the mission, operators diagnose faults and replace parts and subcomponents from available spares. Team leaders ensure Soldiers conduct operator-level preventive maintenance according to the technical manual maintenance allocation chart.

Driver Training

6-66. Driver training qualifies Soldiers to operate the team's assigned vehicle. Signal teams are expected to conduct operations at night, including tactical movement to and displacement from signal sites. Soldiers must be able to operate vehicles at night, during blackout conditions, and under adverse weather conditions. Soldiers must be proficient in the use of night observation devices. Refer to TC 21-305-2 for more information on driving using night vision devices. Driver training includes—

- Driver responsibilities.
- Laws and regulations.
- Basic operating procedures.
- Emergency response procedures.
- Accident causes and reporting.
- Hazards and safety measures.
- Operation of government vehicles off post.
- Transportation of personnel.
- Maintenance responsibilities and forms.
- Convoy operations.
- Driving using night observation devices.
- Hands-on training.
- Performance road test.
- Driving with trailers.

Weapons Training

6-67. Units conduct individual weapons training and qualification to qualify Soldiers on their assigned weapons. Soldiers who fail to qualify must retrain until they are able to qualify.

Communications Security Training

6-68. Soldiers train to use and protect COMSEC devices and keying material. For more information about COMSEC, refer to ATP 6-02.75. COMSEC training includes—

- Key loading.
- Emergency destruction.

- Over-the-air rekeying.
- Incident reporting.
- Material accountability.

TABLE II – INDIVIDUAL SKILLS TEST

6-69. During table II skill testing, a staff sergeant or above certifies Soldiers' proficiency in the individual skills trained during table I training. Soldiers certify on personnel and equipment tasks.

6-70. During table II certification, Soldiers take an individual skills test that certifies their competence on the supporting tasks necessary to install, operate, and maintain their assigned system. Soldiers must complete the Army Combat Fitness Test, qualify on their assigned weapon, complete role-based cyberspace workforce training, and be recommended by their team leader as proficient in their individual supporting tasks.

PERSONNEL CERTIFICATION

6-71. Soldiers are evaluated on their ability to conduct all of the supporting individual tasks for the system they are assigned. They will be evaluated on individual certifications required to perform their tasks, including—

- Role-based cyberspace workforce certification.
- Individual task proficiency.
- Army Combat Fitness Test qualification.

Role-Based Cyberspace Workforce Certification

6-72. The certifying leader verifies cyberspace workforce certification through the Army Training and Certification Tracking System Website. The certifying leader documents completion according to the unit SOP.

Individual Task Proficiency

6-73. The certifying leader evaluates Soldiers' proficiency in individual common and military occupational specialty tasks. Proficiency is achieved when Soldiers perform a training task to standard.

Common Tasks

6-74. The Soldier's manual of common tasks provides information to plan, prepare, train, and evaluate individual training of warrior tasks. Refer to STP 21-1-SMCT for training and evaluation outlines for common tasks.

Military Occupational Specialty Tasks

6-75. Certifying leaders verify Soldiers' proficiency in the individual tasks that support their team's collective tasks and drills. Evaluation checklists are available on the Army Training Network Website.

Army Combat Fitness Qualification

6-76. Certifying leaders verify the Soldier has passed the Army Combat Fitness Test through the unit training noncommissioned officer. Soldiers who fail the Army Combat Fitness Test are subject to administrative action and retest.

EQUIPMENT CERTIFICATION

6-77. Equipment certification provides a guide to the unit ensuring Soldiers meet proficiency standards. Records of certification are retained for training management purposes. Certifying leaders verify—

- Weapons qualification.
- Vehicle licensing.
- Equipment accountability.

Weapons Qualification

6-78. Soldiers qualify on weapons assigned to their team. Certifying leaders verify weapons qualification through the company training records.

Vehicle Licensing

6-79. Signal teams require at least two licensed drivers for each team vehicle. Certifying leaders verify valid licenses through inspection.

6-80. Conducting drivers training at night requires more detailed planning and additional resources to mitigate risk. Soldiers who have requirements to drive at night using night vision devices will conduct proper train up and qualification with those specific pieces of equipment to mitigate risk and ensure success in gaining expertise. Rehearsals must be conducted first during daylight to orient personnel and then at night to test control procedures and equipment. In order to successfully certify, drivers must—

- Use blackout bypass.
- Use night vision devices.
- Conduct convoy operations at night.

Equipment Accountability

6-81. Table II certification includes verifying accountability of assigned equipment. Certifying leaders conduct hand receipt inspections and equipment layouts to verify equipment accountability.

TABLE III – TEAM TRAINING

6-82. After individual Soldiers complete table II certification, the team can begin training collective tasks and drills. Teams train and rehearse collective tasks and drills based on their assigned equipment and mission.

6-83. Table III is the crawl phase of the overall team certification. During table III training, teams train according to the unit SOP and the training and evaluation outlines for the team's collective tasks and drills. Teams progress from daytime iterations under static conditions to nighttime iterations under dynamic conditions. As the team

demonstrates proficiency in its collective tasks, they conduct some training events in mission oriented protective posture 4. Table III consists of personnel and equipment training. The section sergeant conducts table III training and recommends when teams are ready to progress to table to table IV certification.

PERSONNEL TRAINING

6-84. Team training improves the capabilities of Soldiers in their respective team roles. Section sergeants ensure Soldiers complete—

- Table II certification.
- SOPs training.
- Battle drill training.
- Training reinforcement.

Table II Certification

6-85. Table II individual certification is a prerequisite for table III team training. Leaders verify all team members have completed table II certification before beginning table III training.

Standard Operating Procedures

6-86. SOPs use past lessons and best practices to make the unit more effective. Team members review the unit SOP to ensure they are familiar with unit-specific requirements.

Battle Drills

6-87. Battle drills are collective actions performed without the application of a deliberate decision-making process. A battle drill is initiated on a cue, such as an enemy action or a leader's command. A battle drill provides a reflexive response to a given stimulus. Battle drills require minimal leader orders to accomplish. Synchronization and reaction speed are enhanced when battle drills are identified, and the required reactions are defined in the unit SOP and rehearsed during training.

6-88. A battle drill ensures all participants understand a technique or a specific set of procedures. Throughout unit training and preparation for missions, teams rehearse battle drills. Leaders place priority on drills for actions they anticipate occurring during the operation. Refer to FM 6-0 for more information on battle drills.

6-89. Teams build proficiency by conducting battle drills that focus on collective skills. Battle drills for signal teams consist of—

- Warrior battle drills.
- Crew drills.
- SOP battle drills.

Warrior Battle Drills

6-90. Signal teams must be proficient in all common warrior battle drills. Battle drills are group skills designed to teach a unit to react and survive in common combat situations. Refer to STP 21-1-SMCT for a complete list of warrior battle drills with their

supporting individual warrior tasks. Team leaders must also be proficient in skill level 2 drills in STP 21-24-SMCT. Refer to STP 21-1-SMCT for a complete list of warrior battle drills with their supporting individual warrior tasks. Examples of warrior battle drills important to a retransmission team include—

- React to contact.
- Establish security at-the-halt.
- Perform tactical combat casualty care.
- React to ambush.
  - Near.
  - Far.

Crew Drills

6-91. Crew drills are an effective mechanism to validate and sustain team training. Teams should train and conduct team drills according to the unit's combined arms training strategy or SOP. The unit should implement team certification standards to support the unit's mission and incorporate these standards into their operational planning.

Standard Operating Procedure Drills

6-92. SOP battle drills are similar to SOPs; however, they differ in that battle drills require an immediate response when the trigger is initiated for a given event (or situation). For example, a command post will have an SOP that guides the execution of command post security operations. A battle drill will address the immediate actions required when reacting to an enemy attack or other significant event (FM 6-0).

6-93. SOP drills ensure all team members understand a technique or a specific set of procedures. Examples of SOP drills include—

- Command post.
  - Execute emergency evacuation and relocation of a command post.
  - React to a mass casualty incident.
  - React to indirect fire.
- Emergency COMSEC destruction.
- React to electromagnetic interference or attack.

Training Reinforcement

6-94. Training on collective tasks reinforces individual task training. Reinforcement training of collective tasks should be performed to standard through continual training.

EQUIPMENT

6-95. Section sergeants conduct equipment training on the team's assigned equipment. Equipment training includes—

- Team collective tasks.
- Supply discipline.
- Operator maintenance.
- Load plans complete.

Team Collective Tasks

6-96. A collective task requires participation from each team member acting in concert to accomplish the team's assigned mission. A complete training and evaluation outline for each team collective task is available on the Army Training Network Website.

Supply Discipline

6-97. Team leaders train team members in supply discipline procedures. Supply discipline training includes—

- Proper use of equipment.
- Safeguarding government property.
- Inventory techniques.
- Hand receipt procedures.

Operator Maintenance

6-98. Signal teams and operators perform preventive maintenance checks and services on their assigned equipment. Based on the mission, teams and operators diagnose faults and replace parts and subcomponents from available spares. Team leaders train Soldiers to conduct operator-level preventive maintenance according to technical manual maintenance allocation charts.

Load Plan Complete

6-99. Vehicle load plans are based on equipment that is needed first and readily accessible. Section sergeants inspect load plans to ensure teams carry what is necessary for the mission. Standardized load plans allow the platoon leader and platoon sergeant to quickly check accountability of equipment and standards during pre-combat checks and pre-combat inspections.

TABLE IV – TEAM CERTIFICATION

6-100. Soldiers must complete table III training before attempting table IV team certification. During table IV team certification, a sergeant first class or above certifies the team's proficiency in personnel and equipment tasks.

6-101. During table IV certification, teams are certified on the execution of collective and supporting individual tasks. The certification begins with site occupation and consists of day and night iterations. During certification, the team must complete deployment readiness exercise level I, perform preventive maintenance checks and services, and submit DA Form 5988-E for their assigned system.

PERSONNEL TASKS

6-102. Team certification validates Soldiers' ability to perform their respective team roles. A sergeant first class or above certifies teams in—

- Unit-specific requirements.
- Day and night iterations.
- Minimal distractions.
- Deployment readiness exercise.

Unit-Specific Requirements

6-103. Sections complete certification using training and evaluation outlines or the unit SOP. Examples of unit-specific training requirements include—

- Unit-specified time standards.
- Location.
- Mission oriented protective posture conditions.
- Operational environment.
- Reporting requirements.

Day and Night Iterations

6-104. Teams perform tasks in day and night iterations according to unit specific requirements for certification listed in table IV. Certifying leaders evaluate teams during day and night iterations.

Minimal Distractions

6-105. Teams train and certify on tasks with minimal distractions. Leaders safeguard their organization's approved training from external influences that potentially disrupt training.

Deployment Readiness Exercise

6-106. Unit commanders conduct deployment readiness exercises. Leaders ensure movement requests and equipment documentation is complete. Deployment readiness exercise level I evaluates a unit's ability to—

- Alert and assemble the unit.
- Conduct Soldier readiness tasks.
- Verify appropriate deployment certification.
- Verify appointment orders.

Note. Refer to AR 525-93 and AR 600-08-101 for details on conducting deployment readiness exercises.

EQUIPMENT TASKS

6-107. Certifying leaders verify the team proficiency in equipment-related tasks. Equipment certification includes—

- Team collective tasks.
- Maintenance and service verification.
- Hand receipt verification.
- Load plan stressed.

Team Collective Tasks

6-108. Certifying leaders verify the team's collective tasks are trained to proficiency. Each task is evaluated based on the training and evaluation outline. Collective task proficiency is rated as—

- Trained.
- Practiced.
- Untrained.

Maintenance and Service Verification

6-109. Unit maintenance personnel verify all annotated faults on the DA Form 5988-E and order any parts required to resolve faults. Leaders monitor status of ordered parts by verifying entry into the Standard Army Maintenance System-Enhanced.

Hand Receipt Verification

6-110. During table IV certification, hand receipt holders verify accountability of assigned equipment. Certifying leaders annotate discrepancies and notify unit supply personnel of shortages. Unit supply personnel review all sub hand receipts for accuracy before signing.

Load Plan Stressed

6-111. During table IV certification, certifying leaders verify team load plans developed during table III training. Correctly developed load plans enable teams to quickly acquire needed items during certification. Figure 6-3 on page 124 illustrates signal assessment tables I–IV.

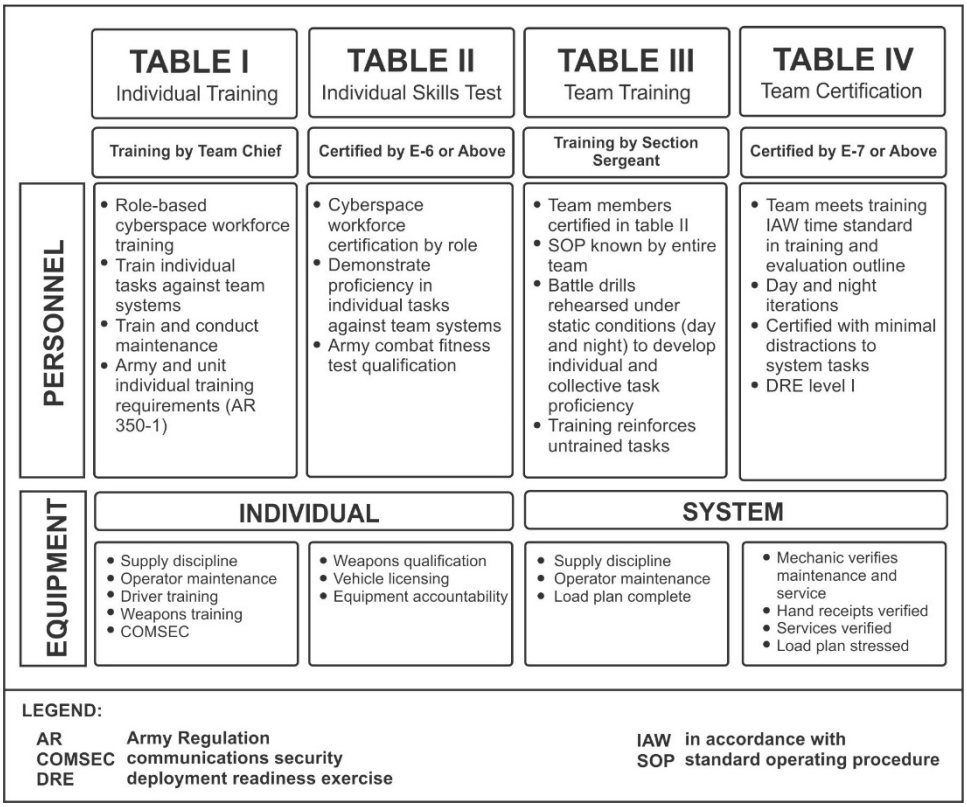


Figure 6-3. Signal assessment tables I–IV

TABLE V – SECTION TRAINING

6-112. During table V training, signal teams combine into sections to train on collective and supporting tasks necessary to establish their node. Sections rehearse battle drills under advanced operational environment conditions, including day and night training, advanced mission oriented protective posture levels, cyber or electromagnetic attack threats, and casualty procedures.

PERSONNEL TRAINING

6-113. Military training improves the capabilities of Soldiers in their respective roles. Platoon sergeants ensure Soldiers complete training in—

- Role-based cyberspace workforce training.
- Individual task training.
- Preventive maintenance.
- AR 350-1 training requirements.

TABLE IV CERTIFICATION

6-114. Before table V training, Soldiers are certified in their ability to conduct the collective tasks and drills for their assigned system.

STATIC TO DYNAMIC BATTLE DRILLS

6-115. Crews develop and train according to SOPs and battle drills during day and night iterations under static conditions. Teams rehearse and train on their battle drills and table of organization and equipment individual and collective tasks. Teams build proficiency by training on battle drills that focus on individual and collective skills and equipment readiness. The training begins with site occupation and consists of day and night iterations.

Training Reinforcement

6-116. Training on the collective tasks reinforces individual task training. Reinforcement training of collective tasks should be performed to standard through continual training.

Employ Teams

6-117. Employing systems in training allows leaders to identify the systems that most reliably support the unit's organic mission, test different methods of employment, develop running estimates, and refine the unit's tactical SOP. Employing systems in training may also allow leaders to identify gaps in support that may drive a request to change the unit's modified table of organization and equipment or submission of an operational needs statement. Training should progress to include simulated cyber and electromagnetic attacks and denied electromagnetic spectrum access to stress the unit's PACE plan.

Operation Order and Troop Leading Procedures Training

6-118. Troop leading procedures provide commanders a framework for planning and preparing for missions. Smaller units—company and below—lack formal staffs and use troop leading procedures to plan and prepare for operations.

6-119. During table V training, the commander trains subordinate platoon leaders and platoon sergeants to plan platoon operations using troop leading procedures. See chapter 3 for detailed information about troop leading procedures in signal companies and platoons.

Communications Security Procedures

6-120. End users protect COMSEC material under their control, and report anything that could jeopardize the COMSEC material. Users follow the COMSEC account manager's instructions for protecting and controlling COMSEC material. COMSEC training includes—

- Key loading.
- Emergency destruction.
- Over-the-air rekeying.
- Incident reporting.
- Material accountability.

6-121. The unit SOP provides local procedures for safeguarding and controlling COMSEC material. All personnel who possess, handle, operate, maintain, or repair COMSEC material must follow physical security and cryptographic security policies and procedures. Refer to ATP 6-02.75 for more information about COMSEC procedures.

EQUIPMENT

6-122. Units conduct individual equipment training and qualification to certify Soldiers on their assigned equipment. Equipment training includes—

- Supply discipline.
- Operator maintenance.
- Driver training.
- Weapons training.
- Communications security.

6-123. The sections will validate the equipment is grouped in the Global Combat Support System-Army as a system of systems in coordination with the unit supply team.

System Group Validation

6-124. Army equipment is identified as systems, subsystems, equipment end items, or a components. Systems are groups of items separately authorized on a modification table of organization and equipment or table of distribution and allowances that form single operational units on their assigned equipment (DA PAM 750-8).

6-125. Subsystems are separately authorized and issued or intended to work with other items to form an operational unit. Components are integral parts of a system, a subsystem or an equipment end item and not authorized separately.

TABLE VI – SECTION CERTIFICATION

6-126. The purpose of table VI is to certify sections are prepared to establish nodes in support of large-scale combat operations. This certification requires sections to complete training and evaluation outline collective drill requirements within the designated time standard, the training event OPORD, and the unit SOP. Sections complete the evaluation for certification during unit collective training events that include dynamic operational environment variables.

6-127. Evaluators conclude their evaluations with checks of unclassified and classified web application access and voice and video checks. Battalion and squadron commanders or their designated representatives certify signal sections.

6-128. Sections are certified to at least table VI before warfighter exercises, combat training center rotations, or comparable culminating training events. Sections, at a minimum, should certify as deployment response exercise level II. table VI certification is conducted semiannually.

PERSONNEL CERTIFICATION

6-129. Soldiers are certified on their ability to conduct all the supporting individual and collective tasks and drills for their assigned system. They are resourced and certified for other individual certifications required to perform their tasks.

Day and Night Iterations

6-130. Teams perform tasks in day and night iterations according to unit specific requirements for certification listed in table IV. The battalion commander or designated representative certifies day and night iterations.

6-131. Sections complete certification using training and evaluation outlines or the unit SOP. Sections perform tasks and drills in day and night iterations according to unit-specific requirements for certification listed in table IV. Battalion commanders or their designated representatives certify the sections. Examples of unit-specific training requirements include—

- Unit-specified time standards.
- Location.
- Mission oriented protective posture conditions.
- Operational environment.
- Reporting requirements.

Network Services

6-132. Sections conduct certification on all supporting individual tasks and drills for their assigned systems. Evaluators certify sections on all tasks and drills according to the unit SOP or training and evaluation outlines. Evaluators verify sections by ensuring—

- Non-classified and classified voice communications tests have been completed.
- Non-classified and classified video teleconferencing tests have been completed.
- Non-classified and classified data communications tests have been completed.

Unit Collective Training Event

6-133. Sections conduct certification during unit training events scheduled by the commander. Commanders ensure all dynamic operational environment variables are established and evaluators certify sections in accordance with the unit SOP or training and evaluation outlines.

Dynamic Operation Environment

6-134. Table VI certification requires dynamic operational environment variables. Dynamic operational environment variables imply that one or more of the operational variables and the opposing force disposition change during execution. The commander validates tactics, techniques, and procedures by successfully executing multiple iterations of a task while constantly adjusting for changes in the operational environment.

Department of Defense Information Network Operations Reporting

6-135. Sections going thorough certification should be able to successfully report network incidents through the network operations and security center. Reporting procedures should be specified in the unit SOP. Evaluators certify sections after verifying reports with the network operations and security center.

Operation Orders

6-136. OPORDs communicate the scope of the training, how to conduct the event, and the tasks to train and evaluate. Successful training events require all leaders to understand the expected training outcome, based on the commander's intent and objectives. OPORDs also ensure subordinates have the information needed to execute the training event. Through the OPORD, the commander clearly identifies the tasks to be trained, the training objectives, and a clearly understandable mission statement.

Exercise Equipment

6-137. The dynamic operational environment should be built to employ all of the section's equipment (radio, switching, line of sight, TROPO, and SATCOM). Evaluators certify sections if all equipment is employed and evaluated according to the training and evaluation outlines. All crews and systems are evaluated and certified during the same event.

Deployment Readiness Exercise Level II

6-138. Unit commanders conduct deployment readiness exercises. Leaders ensure movement requests and equipment documentation is complete. A deployment readiness exercise level II includes level I tasks and is designed to evaluate a unit's ability to conduct complete loadout operations and installation turn-in activities that support a limited notice deployment. Actual packing of a representative sample of the overall unit onto transportation platforms should be accomplished, but installation turn-in can be simulated. A level II deployment readiness exercise includes—

- Alerting and assembling the unit.
- Loading containers and inspecting documentation, including hazardous materials.
- Procuring blocking, bracing, packing, crating, and tie-down materials for containerization.
- Preparing vehicles for all modes of travel and inspecting documentation, including marking and weighing.
- Executing local or internal area movement request procedures for buses, baggage trucks, and material handling equipment support.
- Conducting convoy movement to support the deployment plan.
- Submitting a commander-approved unit deployment list for entry into the Computerized Movement Planning and Status System by the installation transportation office.
- Conducting Soldier readiness tasks.
- Verifying appropriate deployment certification.

Table VI Prior to Training Center Rotation

6-139. Sections are certified through table VI before participating in warfighter exercises, combat training center rotations, or comparable culminating training events. Sections are decertified based on manning thresholds in the unit SOP.

EQUIPMENT CERTIFICATION

6-140. Equipment certification provides a guide to the unit to ensure sections meet proficiency standards. Records of certification are retained for training management purposes. Certifying leaders verify—

- DA 5988-Es.
- Hand receipts.
- Services.
- Load plans.

Maintenance and Service Verification

6-141. Unit maintenance personnel verify all annotated faults on the DA Form 5988-E and order any parts required to resolve faults. Leaders monitor status of ordered parts by verifying entry into the Global Combat Support System-Army.

Hand Receipt Verification

6-142. During table VI certification, hand-receipt holders verify accountability for assigned equipment. Certifying leaders annotate discrepancies and notify unit supply personnel of shortages. Unit supply personnel review all sub hand receipts for accuracy before signing.

Load Plan Verification

6-143. During table VI certification, certifying leaders verify section load plans developed during table III training. Correctly developed load plans enable teams to quickly access needed items during certification.

TABLE VII – SECTION VALIDATION

6-144. Table VII validation is conducted annually. Sections must have certified table VI before attempting table VII. During table VII, sections integrate with multi-echelon training such as warfighter exercises, combat training center rotations, or brigade-level field training exercises to provide signal support. External evaluators or observer, coach, trainers should observe sections.

6-145. Sections are evaluated against the unit's OPORD, SOP, and unit time standards. Table VII evaluates whether the section can effectively support the unit commander. Table VII serves as the training bridge that aligns the training of signal sections and teams with unit and staff training on command and control information systems.

PERSONNEL TRAINING

6-146. Section training improves the capabilities of Soldiers in their respective team roles. Evaluators ensure Soldiers, teams, and sections complete certification in—

- Table VI.
- SOP.
- Drills.
- Training reinforcement.

Table II, IV and VI Certification

6-147. Table VI certification is a prerequisite for table VII evaluation. Leaders verify all team members have completed table VI certification before beginning table VII evaluation.

Signal Support Integration

6-148. A section may achieve table VII validation when they are able to integrate and provide network support to supported units. Evaluators validate sections based on combat training center standards.

Culminating Training Event

6-149. Sections validate at a culminating training event such as a warfighter exercise, combat training center rotation, or brigade field training exercise to which they provide signal support. Sections are be evaluated against the unit's OPORD, SOP, unit time standards, combat training centers standards.

Validation

6-150. External evaluators or observer, coach, trainers validate sections. The evaluation should be validated at multi-echelon training such as a warfighter exercise or combat training center environment.

Deployment Readiness Exercise Level III

6-151. A level III deployment readiness exercise includes level II activities and is designed to evaluate a unit's ability to conduct strategic movement by air or surface in support of a short-notice deployment. A level III deployment readiness exercise includes—

- Preparation of the unit for deployment to participate in designated training.
- After completing Soldier readiness processing, the unit deploys, executes its training mission, and redeploys to its home station.
- Units ensure a commander-approved unit deployment list is used. For example, the deployment list prioritizes personnel and equipment for the advance party.
- If only unit equipment is moving by surface or is loaded for strategic sealift, the unit will still follow the procedures for air movement of passengers, short of the actual allocation of aircraft, if not part of the training scenario.
- Scenarios used in level III deployment readiness exercises reflect the expected types of unit contingency missions and deployment modes.

Dynamic or Complex Operational Environment

6-152. Table VII validation requires dynamic and complex operational environment variables. What makes these variables complex, is when four or more operational or mission variables influence military operations or have a direct or secondary effect on the outcome of military actions. Both the opposing force and training unit leaders must contend with the same variables. The commander validates tactics, techniques, and procedures by successfully executing multiple iterations of a task while constantly adjusting for changes in the operational environment and making the best use of resources.

Department of Defense Information Network Operations Integration

6-153. The network is integrated by planning, establishing, and maintaining the local area networks, wide-area networks, and tactical radio networks. Sections validate by integrating network transport links with networking capabilities. Evaluators validate sections'—

- Communications planning.
- Network management.
- Enterprise systems management.

All Assigned Systems in Use

6-154. Sections are validated in a dynamic or complex operational environment to stress all of the section's radio, switching, line of sight, beyond line of sight and SATCOM equipment. Evaluators validate sections if all equipment is used and evaluated in accordance with the unit SOP or combat training center standards. All crews and systems must certify during the same culminating event.

End Users Supported

6-155. To successfully validate, sections must support end users with a load on the network. Evaluators validate sections once the network successfully passes data under stress with non-classified and classified voice, data, and video communications.

EQUIPMENT

6-156. Equipment validation provides a guide to the commander ensuring section proficiency. Validation records are retained for training management purposes. External evaluators or observer, coach, trainers conduct the validation. Certifying leaders validate the following tasks for the nodes—

- DA 5988-Es verified.
- Hand receipts verified.
- Services verified.
- Load plan stressed.

Maintenance and Service Verification

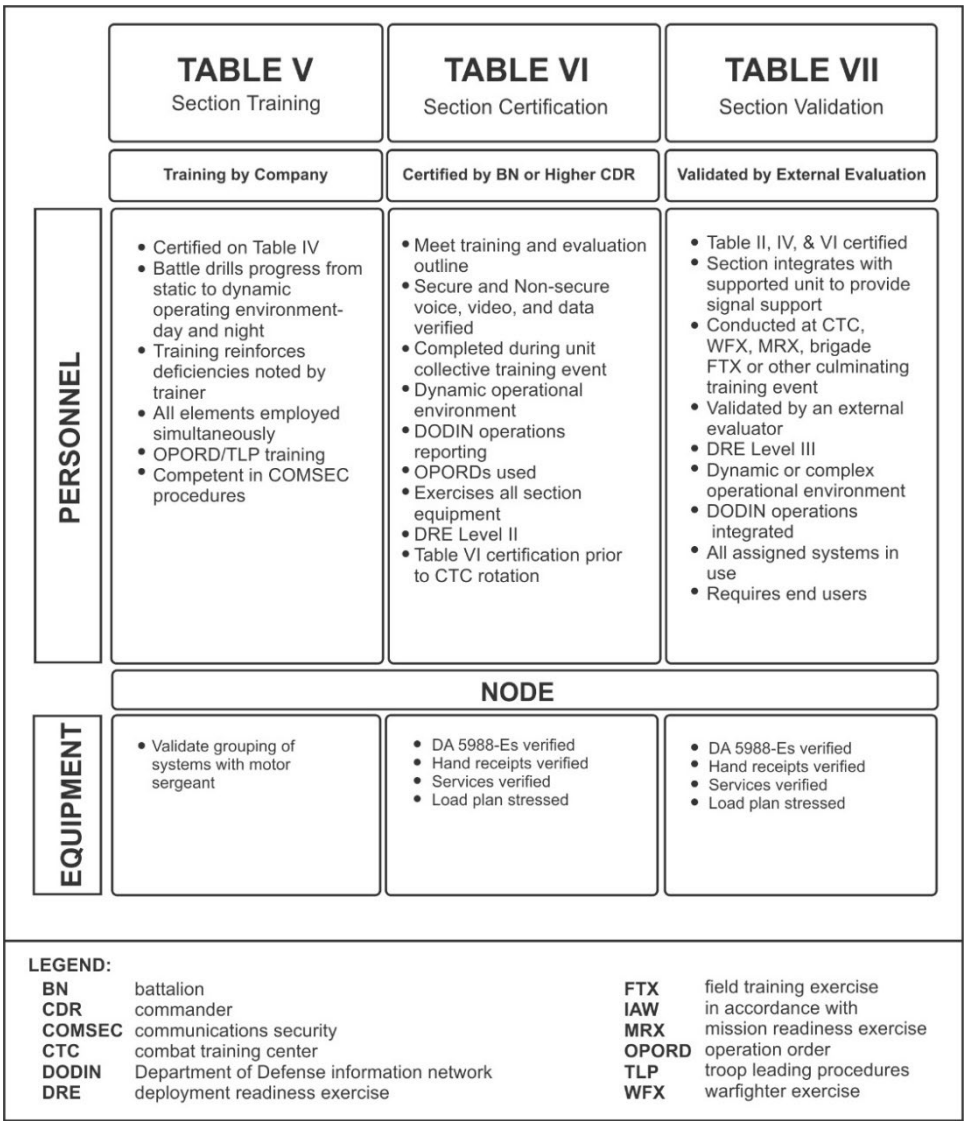
6-157. Unit maintenance personnel verify all annotated faults on the DA Form 5988-E and order any parts required to resolve faults. Leaders monitor status of ordered parts by verifying entry into the Global Combat Support System-Army.

Hand Receipt Verification

6-158. During table VII validation, hand-receipt holders verify accountability for assigned equipment. Certifying leaders annotate discrepancies and notify unit supply personnel of shortages. Unit supply personnel review all sub hand receipts for accuracy before signing.

Load Plan Stressed

6-159. During table VII validation, certifying leaders verify team load plans developed during table III training. Correctly developed load plans enable teams to quickly access needed items during the culminating event. Figure 6-4 on page 133 illustrates signal assessment tables V–VII.



1009 **Figure 6-4. Signal assessment tables V–VII**

This page intentionally left blank.

Appendix A

Recognizing and Responding to Cyber and Electromagnetic Warfare Attacks

This appendix addresses the means to recognize and overcome threat activities affecting signal support in a contested environment. It includes an overview of peer threat tactics, techniques, procedures, and methods to counter threat cyber and electromagnetic attacks. Refer to ATP 3-12.3 for more information on electromagnetic warfare.

THREAT TACTICS, TECHNIQUES, AND PROCEDURES

A-1. A peer threat's information warfare activities will integrate electromagnetic attack, military deception, lethal fires, perception management, information attack, and computer warfare to deny U.S. and allied forces access to the electromagnetic spectrum in a contested environment.

A-2. Understanding threat capabilities in the electromagnetic spectrum is key to sound signal support plans. Enemy attacks on friendly command and control nodes may combine electromagnetic attacks, other information warfare effects, and lethal fires to deny friendly forces the use of spectrum-dependent systems. To accomplish this goal, threat forces gather technical and combat information about their enemies. As enemy forces locate and identify friendly units, enemy information warfare elements establish priorities to—

- Jam communications assets.
- Deceptively enter radio networks.
- Interfere with the normal flow of U.S. and allies' communications.

MEASURES TO PREVENT THREAT EFFECTS

A-3. Understanding threat capabilities is critical to hardening the deployed network against enemy EW and signals intelligence. If an enemy cannot detect command posts and communications sites, it cannot target the sites with electromagnetic attack or lethal fires.

LIMITING ELECTROMAGNETIC SIGNATURE

A-4. To protect against a peer threat's ability to locate and target radio signals, the S-3 must plan signal support in a way that limits the electromagnetic signature of command posts. Measures to reduce the electromagnetic signature of command posts and communications sites include—

- Careful siting of radio equipment.
- Employment of directional antennas.
- Operations using lowest power required.
- Limiting radio transmissions.
- Using a random schedule.

A-5. Electromagnetic protection techniques can also help mask the electromagnetic signature. The cyber electromagnetic warfare officer can assist the S-3 in planning electromagnetic protection measures to reduce the command post electromagnetic signature.

TERRAIN MASKING

A-6. Terrain masking can effectively block radio signals from reaching enemy direction-finding capabilities. Positioning communications systems with large terrain features or manmade structures between the communications system and the forward line of own troops effectively blocks an enemy from detecting the signal.

CAMOUFLAGE NET MASKING

A-7. Radar reflective camouflage netting is an effective means of blocking stray electromagnetic radiation from directional antennas. Camouflage netting placed to the sides and back of a line of sight or SATCOM antenna ensures only the main beam of the antenna radiates. Since the main beam is directional, it is much harder for the enemy to detect; the enemy would need to be directly in the transmission path.

LINE OF SIGHT

A-8. High-throughput line of sight radios can carry high bandwidth data over distances up to 40 kilometers (25 miles). Planners should engineer links to minimize chances of detection, targeting, and jamming. If the line of sight path is parallel to the forward line of own troops, an enemy is less likely to detect the signal, and enemy jammers cannot reach the antenna with a strong enough signal to jam the radio.

REMOTE ANTENNAS

A-9. Large command posts and high-throughput communications systems emit a significant amount of electromagnetic energy. Planners and operators can mask some of this energy with directional antennas, site selection, terrain masking techniques, but some energy remains. Because command and control capabilities are a priority target for peer threats, anything near the communications system is at risk of destruction from lethal fires.

A-10. Commanders and signal planners should consider locating major communications assemblages as far from the supported command post as practical. Selecting a site with terrain features, manmade structures, or distance between communications systems and command posts protects the command post from lethal fires. Commanders and planners must consider the additional physical security and site defense requirements for a remote site during planning.

FREQUENT COMMAND POST DISPLACEMENT

A-11. Despite efforts to reduce and mask the electromagnetic signature of a command post, a peer threat may eventually locate it. Moving a command post frequently reduces its chance of destruction. This is especially important when operating within the range of enemy long range fires. Peer threats are able to mass lethal fires to destroy an area target quickly. During training exercises, units must practice frequent command post displacement and handover between the main and tactical command posts.

A-12. Leaders should focus command posts on the minimum functions necessary to retain their mobility and do everything possible to avoid detection. When the risk of enemy fires is high, commanders consider making their operations more decentralized, dispersing command post nodes into smaller component nodes, and greater dispersion of electromagnetic signatures (FM 3-0).

SATELLITE SITE SELECTION AND RADIO FREQUENCY INTERFERENCE

A-13. SATCOM systems suffer from natural and manmade interference. Natural sources of interference include solar activity, dense vegetation, thick cloud cover, heavy precipitation, and sandstorms. Manmade sources of interference include vehicles, buildings, and other structures that obstruct the line of sight path to the satellite, jamming, and radio frequency interference.

A-14. Commanders and staffs need to identify and minimize the command post footprint and electromagnetic signature. Planners and operators should identify physical surroundings to minimize interference and mask the electromagnetic signatures of deployed communications systems. Refer to ATP 6-02.70 for more information on radio frequency interference.

A-15. Signal elements operating from locations without masking terrain features or structures can use power settings and radio frequency management techniques, to control interference and detection. When establishing satellite links, the equipment operator should communicate with satellite network controllers to determine the minimum required power level. Using a higher power signal than needed for communications increases the likelihood an enemy detection and targeting of the communications capability. Refer to ATP 6-02.53 and ATP 3-12.3 for more information on masking and power settings.

RECOGNIZING AND RESPONDING TO THREAT EFFECTS

A-16. Because peer threats consider friendly command and control capabilities to be high priority targets, they have developed capabilities to deny their enemies the effective use of the electromagnetic spectrum for communications. Signal Soldiers and leaders must learn to identify and respond to threat effects in cyberspace and the electromagnetic spectrum.

ELECTROMAGNETIC SPECTRUM (JAMMING)

A-17. *Electromagnetic jamming* is deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, with the intent of degrading or neutralizing the enemy's combat capability (JP 3-85). Jamming is an effective way for the enemy to disrupt friendly communications. An enemy only needs a transmitter tuned to a U.S. frequency with enough power to overpower friendly signals to effectively jam U.S. systems.

A-18. Jammers operate against receivers, not transmitters. The two modes of jamming are spot and barrage jamming. Spot jamming concentrates power on one channel or frequency. Barrage jamming is power spread over several frequencies or channels at the

same time. It is important to recognize jamming, but it can be difficult to detect. Refer to ATP 3-12.3 and ATP 6-02.53 for more information about electromagnetic jamming.

Communications Jamming

A-19. Radio operators must learn to recognize and react to electromagnetic jamming. This is not always an easy task since electromagnetic interference can be either internal or external. Other sources having nothing to do with enemy jamming may cause electromagnetic interference. Unintentional electromagnetic interference may be caused by—

- Other radios (friendly and enemy).
- Other electronic, electrical, or electromechanical equipment.
- Atmospheric conditions.
- Equipment malfunction.

A-20. Radio operators must train to differentiate internal and external interference quickly. Electromagnetic jamming most commonly affects single-channel radio systems. These radios include HF, VHF, and UHF radios. Jamming effects may be obvious or subtle. Obvious jamming is normally simple to detect. When experiencing jamming, it is more important to recognize and overcome the incident than to identify it formally.

A-21. Subtle jamming is less obvious because subtle jamming signals produce no sound from the receivers. Although everything may appear normal to the radio operator, the receiver cannot receive an incoming friendly signal. Often, users assume their radios are malfunctioning, instead of recognizing subtle jamming. Table A-1 on page 139 lists and describes the characteristics of some common jamming signals.

146 **Table A-1. Common jamming signals**

Signal	*Description*
Random Noise	Synthetic radio noise. It is indiscriminate in amplitude and frequency. It is similar to normal background noise and can degrade all types of signals. Operators often mistake random noise jamming for receiver or atmospheric noise and fail to take appropriate electromagnetic protection actions.
Stepped Tones	Tones transmitted in increasing and decreasing pitch. They resemble the sound of bagpipes. Stepped tones are effective against single-channel amplitude modulation or frequency modulation voice circuits.
Spark	Bursts are of short duration and high intensity; they are repeated at a rapid rate. This signal is effective in disrupting all types of radio communications. Spark jamming is easy to produce and one of the most effective jamming signals.
Gulls	Quickly rising and slowly falling variable radio frequency. The effect produced is similar to the cry of a seagull. Gulls produce a nuisance effect and are very effective against voice radio communications.
Random Pulse	Pulses of varying amplitude, duration, and rate. Pulses disrupt teletypewriter, radar, and various data transmission systems.
Wobbler	A single frequency, modulated by a low and slowly varying tone. The result is a howling sound that causes a nuisance effect on voice radio communications.
Recorded Sounds	Any audible sound, especially of a variable nature. Recorded sounds can distract radio operators and disrupt communications. Music, screams, applause, whistles, machinery noise, and laughter are examples.
Preamble Jamming	A tone resembling the synchronization preamble of the speech security equipment, broadcast over the operating frequency of secure radio sets. Results in all radios being locked in the receive mode. Preamble jamming is especially effective when employed against radio networks that use speech security devices.

147 ***Preventive Measures***

148 A-23. Measures operators and planners can use to reduce susceptibility to enemy
149 jamming include—

150 • Minimizing radio transmissions—users should try to keep radio transmissions
151 to six seconds or less.
152 • Using electromagnetic counter-countermeasures, such as frequency hopping.
153 • Training using radio silence.
154 • Using low power setting on radios for normal operations to reduce the
155 probability of detection.
156 • Using terrain masking to reduce the probability of detection and block potential
157 sources of enemy jamming.

Indicators

A-24. The enemy strives to perfect and use new and more confusing forms of jamming, which requires radio operators to be increasingly alert to the possibility of jamming. Training and experience allow operators to determine whether a particular signal is a jamming signal. During operations, radio operators should remain alert to possible jamming indicators. Observable indications of jamming include—

- Apparently random noise or static over voice channels.
- Recorded sounds—messages or music—over voice channels.
- No answer to a radio transmission.

Reaction

A-25. Communications jamming requires prompt corrective action to restore critical communications capabilities. Possible reactions to jamming include—

- **Continuing to operate**—Enemy jamming usually involves a period of jamming followed by a brief listening period. Operator activity during this short period indicates to enemies whether their jamming efforts were successful. Continuing to operate normally gives the enemy no indication of success for failure. If the enemy hears discussion of the problem on the air, or radio operation terminates, the enemy may assume their jamming is effective. Operators should never terminate operation of a radio network unless ordered to do so. Operators should be careful not to disclose adverse effects of enemy jamming. This means normal operations should continue even when degraded by jamming.
- **Increasing transmitter power output**—Using low power for normal operations minimize the chance of detection. Once the enemy begins jamming the radios, the risk of detection becomes secondary to the radio delivering required communications. Higher radio power may overcome the enemy's jamming signal but increases the risk of detection by enemy direction-finding capabilities.
- **Improving the Signal-to-Jamming Ratio**—The signal-to-jamming ratio is the relative strength of the desired signal to the jamming signal at the receiver. If the desired signal is much stronger than the jamming signal, the jamming does not significantly degrade communications. To improve the signal-to-jamming ratio operators and signal leaders can consider—
  - **Adjusting or changing the antenna—**When jamming occurs, the radio operator should adjust the antenna to receive the maximum incoming signal strength. Depending on the antenna, some methods include reorienting the antenna, changing antenna polarization at all stations, or installing an antenna with a greater range.
  - **Establishing a retransmission site**—A retransmission site can increase the effective range and power of a signal between radio stations without increasing transmit power.
  - **Relocating the antenna**—Operators may use terrain masking to block the incoming jamming signal. This may require relocating the antenna and associated radio set up to several hundred meters from its previous location.

- **Changing frequencies**—If a communications network cannot overcome enemy jamming, the commander may direct use of an alternate or spare frequency. Preplanned and well-coordinated actions are required in order for practical dummy stations to continue to operate on the jammed frequency, to mask the change to an alternate frequency. During a jamming incident, it may be difficult to coordinate a frequency change. All radio operators require knowledge of when, and under what circumstances, they should switch to a backup frequency. If the frequency change is not smooth, the enemy may discover what is happening, and try to degrade communications on the new frequency.
- **Executing the PACE plan**—Quickly changing to the alternate or contingency means of communications reduces disruption of the command and control system.
- **Using signals intelligence or EW capabilities to locate the jamming signal**—Leveraging signals intelligence or EW capabilities requires coordination and collaboration with the S-2 or the cyber electromagnetic warfare officer.

A-26. If any of the corrective actions taken mitigate the enemy jamming, operators should continue operation of the network and submit a joint spectrum interference resolution report to the higher headquarters spectrum manager. This can be done through the joint Spectrum Interference Resolution Online Portal, accessed through SECRET Internet Protocol Router Network by spectrum managers. Joint spectrum interference resolution reports document a history of problems and help identify possible causes for subsequent interference. Maintaining a historical record of interference helps develop countermeasures to future jamming incidents. Refer to ATP 6-02.70 for more information about joint spectrum interference resolution reporting and Joint Spectrum Interference Resolution Online.

Positioning, Navigation, and Timing Jamming

A-27. Peer threats have capabilities to contest the space domain and attack the on-orbit, link, and terrestrial segments of U.S. positioning, navigation, and timing satellites. These attacks may have significant impacts across all warfighting functions and many weapon platforms.

A-28. Electromagnetic jamming of positioning, navigation, and timing satellite capabilities affects not only communications, but also many other capabilities in tactical formations. Systems affected include—

- Communications systems.
- Friendly force unmanned aircraft system tracking.
- Navigation.
- Reconnaissance.
- Radar systems.
- Precision-guided munitions.

Preventive Measures

A-29. Measures to reduce susceptibility to, and mitigate the effects of, enemy jamming of positioning, navigation, and timing include—

- Using only encrypted positioning, navigation, and timing systems.
- Antenna masking.
- Terrain masking.
- Training and maintaining the ability to navigate using a map and compass.

Indicators

A-30. User indications that an enemy may be jamming positioning, navigation, and timing satellites include—

- Loss of satellite signal.
- A red Global Positioning System icon on the network management system.
- Loss of timing or incorrect time displayed on equipment.
- Wrong location displayed on the map.
- Jamming environment warning message.

Reaction

A-31. Because of the diverse and widespread effects of enemy positioning, navigation, and timing jamming, a prompt, coordinated response is necessary. Operators of affected systems should—

- **Navigate using map and compass**—While this does not restore system timing and situational awareness displays, navigation using a map and compass cannot be jammed.
- **Increase distance between affected systems and jammer**—If the jammer operates from a known location, increased distance or terrain masking may mitigate interference.
- **Use signals intelligence or EW capabilities to locate the jamming signal**—Leveraging signals intelligence or EW capabilities requires coordination and collaboration with the S-2 or the cyber electromagnetic warfare officer.
- **Report jamming to higher headquarters**—Submitting a joint spectrum interference resolution report to higher headquarters documents a history of problems and helps identify possible causes for subsequent interference.

Satellite Communications Jamming

A-32. Expeditionary forces rely heavily on SATCOM capabilities for beyond line of sight network transport. Systems and capabilities affected by SATCOM jamming include—

- Friendly force tracking.
- Command post information systems.
- TACSAT radios.
- Intelligence reporting systems.

Preventive Measures

A-33. Operational and employment measures to prevent SATCOM jamming include—

- Minimizing transmissions on narrowband (single-channel) TACSAT radios—users should try to keep radio transmissions to six seconds or less.
- Terrain masking.

- Camouflage net masking.

Indicators

A-34. Possible operator indications of satellite jamming include—

- Seemingly random noise or static on narrowband (single-channel) TACSAT radios.
- Recorded sounds, such as messages or music, over narrowband (single-channel) TACSAT radios.
- No answer to transmission.
- Red satellite icon on network management system display.
- Loss of data from the satellite.
- Low signal-to-noise indicated on a wideband satellite terminal.

Reaction

A-35. The reactive measures here apply mostly to narrowband (single-channel) SATCOM systems. When a narrowband (single-channel) TACSAT radio operator recognizes a jamming attempt, they may—

- **Increase radio transmit power**—Only increase power on wideband SATCOM terminals if directed by the satellite controller.
- **Change to a preapproved alternate frequency.**
- **Execute the PACE plan**—Quickly changing to the alternate or contingency means of communications reduces disruption of the command and control system.
- **Use signals intelligence or EW capabilities to locate the jamming signal**—Leveraging signals intelligence or EW capabilities requires coordination and collaboration with the S-2 or the cyber electromagnetic warfare officer.
- **Report jamming to higher headquarters**—The higher headquarters' frequency manager and cyber electromagnetic warfare officer can correlate reports from units across the assigned area to isolate enemy jammers and plan countermeasures, including nominating targets for lethal fires.
- **Use line of sight systems for network transport**—Units cannot communicate beyond line of sight, or through significant physical obstacles.

A-36. Satellite network controllers at the WSOC coordinate interference resolution and reporting on DOD wideband satellite networks.

JOINT SPECTRUM INTERFERENCE RESOLUTION

A-37. Joint spectrum interference resolution reporting addresses electromagnetic interference and jamming incidents affecting the DOD. The objective of joint spectrum interference resolution is to document and assist in resolving electromagnetic attack and recurring electromagnetic interference.

Incident Resolution

A-38. Spectrum managers and signal and EW Soldiers attempt to resolve incidents at the lowest possible level using organic assets. If the spectrum manager and cyber electromagnetic warfare officer cannot resolve an incident locally, they submit a joint

spectrum interference resolution report through the chain of command. Each successive level attempts to resolve the incident before forwarding the report.

A-39. Corps and division spectrum managers coordinate regional and local interference resolution. The impact of each interference incident is unique, so no standard procedure establishes or guarantees resolution in every case. A systematic approach reduces the time and cost required to resolve interference situations. Refer to ATP 6-02.70 for more information about joint spectrum interference resolution reporting.

Reporting Procedure

A-40. Joint spectrum interference resolution reporting takes place through secure channels. Spectrum managers should not delay reports due to a lack of complete information. They can submit an initial report while attempting to resolve the incident, and follow-up reports to provide additional information, as it becomes available.

A-41. The submitter of a joint spectrum interference resolution report determines the appropriate security classification by evaluating the sensitivity of the electromagnetic interference on the affected system and considering the classification of the text comments.

A-42. Army units report through their chain of command up to the combatant command and the United States Army Communications-Electronics Services Office. Message precedence of a joint spectrum interference resolution report depends on the urgency of the reported situation. Normally reports are routine or priority precedence, unless the originating unit believes the incident is hazardous to military operations. In this case, the unit reports using immediate precedence.

MALICIOUS CYBERSPACE ACTIVITIES

A-43. U.S. networks face continuous risk of malicious cyberspace activities. Cyberspace risk increases substantially when operating against a peer threat in a contested environment. DODIN operations personnel implementing cybersecurity measures can prevent many attacks. If an enemy's malicious cyberspace activity breaches cybersecurity measures, it may require defensive cyberspace operations support to mitigate. Refer to FM 3-12 for more information about defensive cyberspace operations support.

Denial-of-Service

A-44. A denial-of-service attack seeks to make a computer or network resource unavailable to its intended users by disrupting services of a host connected to the Internet. An attacker floods the target computer or network resource with more requests than it can handle to overload the system and prevent it from fulfilling legitimate requests.

A-45. Denial-of-service attacks can affect any Internet Protocol network system, including—

- Command post information systems.
- Logistics systems.
- Administrative systems.

- End user devices.

Preventive Measures

A-46. Good cybersecurity practices can prevent or lessen the effects of a denial-of-service attack. Cybersecurity personnel should—

- Maintain current antivirus software and virus definition files.
- Maintain properly configured network firewalls.

Indicators

A-47. Operator indications of a denial-of-service attack may include—

- Unusually slow network performance when opening files or accessing websites.
- Request timeouts.
- Widespread unavailability of a website or network system.

Reaction

A-48. When faced with the symptoms of a denial-of-service attack, DODIN operations personnel should—

- Report to the next higher echelon S-6, G-6, or J-6 to determine whether the system slowdown is due to known activity on the network.
- Report suspected attacks to the S-2 and S-3.
- Continue operations using alternate or contingency communications means.

Malware

A-49. Malware is malicious software intentionally designed to damage a computer, server, or computer network. Malware attacks can affect any automated information system, including—

- Command post information systems.
- Logistics systems.
- Administrative systems.
- End user devices.

Preventive Measures

A-50. Cybersecurity personnel attempt to prevent malware attacks by—

- Using and maintaining up to date antivirus software and virus definition files.
- Keeping system software updated and patched.
- Ensuring compliance with the most recent security technical implementation guides.
- Maintaining properly configured network firewalls.

Indicators

A-51. Possible indicators of a malware attack include—

- Destruction or unexplained changes to files.
- Spontaneous restart of computers.

- Erratic, delayed, or unexpected computer or network activity.
- Antivirus software warnings.

Reaction

A-52. If operators or DODIN operations personnel observe indications of a possible malware attack, they should—

- Report to the next higher echelon S-6, G-6, or J-6.
- Continue operations using alternate or contingency communications means.
- Report to the S-2 and S-3.
- DODIN operations personnel should not reconfigure computers or network systems in response to an attack unless directed by their next higher echelon.

Data Exfiltration and Collection

A-53. Data exfiltration may be either electronic—removing files through the network, or physical—removing paper or electronic copies from sensitive areas. Either method may disclose sensitive operational information and plans. Exfiltration of sensitive data may place operations at risk.

A-54. All automated information systems are potential targets of data exfiltration and collection. Affected systems include—

- Command post information systems.
- Logistics systems.
- Administrative systems.
- End user devices.

Preventive Measures

A-55. Cybersecurity measures and physical security combine to prevent data exfiltration and collection by—

- Implementing strict identity, credential, and access management controls for network systems.
- Enforcing strict physical security controls.
- Implementing access control restrictions.
- Employing data loss prevention software.
- Encrypting data-at-rest.
- Maintaining strong network access controls.

Indicators

A-56. Indicators of enemy data exfiltration and collection efforts include—

- Attempted or successful unauthorized physical access to sensitive areas.
- Unusually high volume of outgoing network traffic.

Reaction

A-57. The effects of data exfiltration can be catastrophic. If an enemy can steal enough documents, they can develop a complete assessment of U.S. capabilities, troop strength,

logistics, and even operation plans. If any member of the unit suspects an enemy data exfiltration attempt, they—

- Report to the S-2 and S-3.
- Report to the next higher echelon.
- Consider changing the maneuver course of action if exfiltration compromises operation or support plans.

Social Engineering

A-58. Social engineering uses techniques that rely on weakness in human nature rather than hardware or software. The goal is to deceive people into revealing passwords and other information that compromise the security of automated information systems and networks. Threats may also use social engineering techniques to identify and develop potential targets for phishing and spear phishing.

A-59. The target of a social engineering attack is an individual. A successful social engineering attack may compromise any system to which the affected individual has access.

Preventive Measures

A-60. All individuals should maintain operations security and cybersecurity awareness to avoid falling victim to a social engineering attack. They should—

- Confirm the identity of persons asking for personal information or access credentials.
- Pay close attention to website addresses.
- Avoid disclosing any information to unknown or unverified persons. Disclosing even seemingly innocuous information could make subsequent social engineering or spear phishing attempts against other targeted individuals seem much more legitimate.

Indicators

A-61. Indicators of social engineering attempts include—

- Unexpected phone calls from unknown callers requesting sensitive information.
- Websites that do not look normal, contain broken links, or have a mismatch between the text link and Internet address.
- Unauthorized personnel shoulder surfing.

Reaction

A-62. If personnel suspect a social engineering attempt, they should—

- Confirm the requestor's identity before disclosing information.
- Report the attempt to supervisors, network managers, and the S-2.
- Report social engineering attempts to next higher echelon.
- Promptly reporting attempts at social engineering can raise awareness and prevent others from falling victim to the same techniques.

Phishing and Spear Phishing

A-63. Phishing is a fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by posing as a trustworthy entity in electronic communications. Spear phishing is a targeted phishing attempt, usually against key individuals or personnel with elevated or special access privileges.

A-64. Any individual may fall victim to a phishing attack. Key leaders and network administrators are also subject to spear phishing.

Preventive Measures

A-65. All personnel should protect themselves from phishing attacks by following best practices outlined in the annual cybersecurity awareness challenge. Depending on the cyber protection condition level, the command may—

- Maintain awareness of the personal use of commercial e-mail.
- Restrict the use of personal e-mail, as required.
- Block access to commercial e-mail providers.

Indicators

A-66. Most common phishing techniques share certain traits, including—

- E-mails with generic greetings. Note that spear phishing attempts are likely be more refined and address the targeted individual by name.
- E-mails requesting personal information or login credentials.
- E-mails requesting or demanding an urgent response.
- E-mails with spoofed links, where the text displayed does not match the Internet address shown when hovering over the link.

Reaction

A-67. If an individual suspects a phishing or spear phishing attempt, they should—

- Report the attempt to the chain of command, automation support section, and the S-2.
- Confirm the identity of the sender before taking any action.
- Individuals can further protect themselves from fraudulent links by never accessing their personal accounts through links in e-mails. For instance, if an e-mail purports to be from the individual's bank or credit card company, they should access their account only through the legitimate secure website, not through a hyperlink provided in an e-mail.

A-68. Commands should not threaten punishment against individuals who inadvertently fall victim to phishing attempts. Fear of punishment could prevent individuals from reporting attacks.

Social Media Attacks

A-69. Threats may conduct social media attacks in support of their information collection and information operations goals. All individuals using any form of social media are potential targets.

Preventive Measures

A-70. Individuals should strictly limit personal information posted to their social media accounts. The compromise of this information could be damaging or could strengthen a threat's subsequent social engineering or spear phishing attacks. To limit vulnerability to social media attacks—

- Individuals should restrict who can view their social media profile and activities using the privacy settings on the social media platform.
- Individuals and public affairs personnel must carefully weigh operations security considerations when they engage on social media platforms.
- Individuals and group administrators should not accept friend or group membership requests from unknown or unverifiable persons.
- Commands should consider limiting or restricting access to social media platforms as mission or operations security concerns dictate.

Indicators

A-71. Indicators of potential social media attacks include—

- Friend requests from unknown persons, or duplicate friend requests that mimic a known person.
- Unknown persons commenting on social media posts.

Reaction

A-72. If a social media attack is known or suspected, personnel should—

- Report the suspected compromise to the S-2.
- Immediately change any compromised passwords.
- Watch for indicators of identity theft.

Attacks Against Personal Electronic Devices

A-73. Widespread use of personal electronic devices creates significant vulnerabilities when operating against a peer threat. Peer threats have demonstrated advanced capabilities to exploit personal electronic devices, seize control of cellular communications networks, and locate personal cellular phones with precision. This gives them the ability to collect information, conduct information warfare activities, and direct accurate lethal fires. Any personal electronic device capable of connecting to Wi-Fi, Bluetooth, or cellular communications systems is vulnerable to attack.

Preventive Measures

A-74. Measures to protect against personal electronic device attacks include—

- Maintaining strict control and accountability of personal electronic devices.
- Downloading only trusted apps from approved sources.
- Maintaining current security updates on devices and apps.
- Disabling Bluetooth and Wi-Fi features when they are not in use.
- Encrypting sensitive files and personal information.
- Allowing only government-provided personal electronic devices to connect to the DOD network.

- Commanders should consider restricting or banning the use of personal electronic devices, based on the tactical situation.

Indicators

A-75. Some possible indicators of attacks against personal electronic devices are—

- Enemy attacks that seem to correlate with personal electronic device usage.
- Incoming lethal fires that occur with unexplained precision.
- Receiving a barrage of text messages—up to several per second—preventing the intended use of the device.
- Incoming propaganda or psychological warfare messages from unknown numbers.

Reaction

A-76. If a unit suspects it has come under attack, commanders should—

- Quickly displace the element under attack and direct all personnel to turn off personal electronic devices.
- Disable personal electronic devices and confiscate them, if necessary.
- Report to the next higher echelon.

Glossary

The glossary lists acronyms and terms with Army, multi-service, or joint definitions, and other selected terms. The proponent for terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

CECOM	United States Army Communications-Electronics Command
COMSEC	communications security
DODIN	Department of Defense information network
DODIN-A	Department of Defense information network-Army
EW	electromagnetic warfare
FRAGORD	fragmentary order
G-3	assistant chief of staff, operations
G-4	assistant chief of staff, logistics
G-6	assistant chief of staff, signal
HCLOS	High Capacity Line of Sight
HF	high frequency
J-3	operations directorate of a joint staff
J-6	communications system directorate of a joint staff
LAN	local area network
MED	medical
METT-TC (I)	mission, enemy, terrain and weather, troops and support available, time available, civil considerations, and informational considerations
OPORD	operation order
PACE	primary, alternate, contingency, and emergency
RSSC	regional satellite communications support center
SATCOM	satellite communications
S-3	battalion or brigade operations staff officer
S-4	battalion or brigade logistics staff officer
S-6	battalion or brigade signal staff officer
SMART-T	Secure Mobile Anti-jam Reliable Tactical Terminal
SOP	standard operating procedure
SPEED	System Planning, Engineering, and Evaluation Device

TACSAT	tactical satellite
TB	technical bulletin
TRILOS	Terrestrial Transmission Line of Sight
TROPO	tropospheric scatter
UHF	ultrahigh frequency
VHF	very high frequency
WARNORD	warning order
WSOC	wideband satellite communications operations center

SECTION II – TERMS

adversary

A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged. (JP 3-0)

avenue of approach

A path used by an attacking force leading to its objective or to key terrain. Avenues of approach exist in all domains. (ADP 3-90)

civil considerations

The influence of manmade infrastructure, civilian institutions, and attitudes and activities of the civilian leaders, populations, and organizations within an assigned area on the conduct of military operations. (ADP 6-0)

classes of supply

The ten categories into which supplies are grouped to facilitate supply management and planning. I. Rations and gratuitous issue of health, morale, and welfare items. II. Clothing, individual equipment, tentage, tool sets, and administrative and housekeeping supplies and equipment. III. Petroleum, oils, and lubricants. IV. Construction materials. V. Ammunition. VI. Personal demand items. VII. Major end items, including tanks, helicopters, and radios. VIII. Medical. IX. Repair parts and components for equipment maintenance. X. Nonstandard items to support nonmilitary programs such as agriculture and economic development. See also petroleum, oils, and lubricants. (JP 4-09)

commander's critical information requirement

Specific information identified by the commander as being essential to facilitate timely decision making. (JP 3-0)

command post

A headquarters, or a portion thereof, organized for the exercise of command and control. (FM 6-0)

communications security

Actions designed to deny unauthorized persons information of value by safeguarding access to, or observation of, equipment, material, and documents with regard to the possession and study of telecommunications or to purposely mislead unauthorized persons in their interpretation of the results of such possession and study. **Also called COMSEC.** (JP 6-0)

concealment

Protection from observation or surveillance. (FM 3-96)

constraint

A restriction placed on the command by a higher command. A constraint dictates an action or inaction, thus restricting the freedom of action of a subordinate commander. (FM 5-0)

cover

Protection from the effects of fires. (FM 3-96)

cyberspace domain

(Army) The interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunication networks, computer systems, embedded processors and controllers, and relevant portions of the electromagnetic spectrum. (FM 3-0)

decisive terrain

Key terrain whose seizure and retention is mandatory for successful mission accomplishment. (ADP 3-90)

Department of Defense information network

The set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone. **Also called DODIN.** (JP 6-0)

Department of Defense information network-Army

An Army-operated enclave of the Department of Defense information network that encompasses all Army information capabilities that collect, process, store, display, disseminate, and protect information worldwide. **Also called DODIN-A.** (ATP 6-02.71).

electromagnetic jamming

The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, with the intent of degrading or neutralizing the enemy's combat capability. (JP 3-85)

electromagnetic masking

The controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy electromagnetic support measures/signals intelligence without significantly degrading the operation of friendly systems. (JP 3-85)

electromagnetic protection

Division of electromagnetic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. (JP 3-85)

emission control

The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors, b. mutual interference among friendly systems and/or c. enemy interference with the ability to execute a military deception plan. **Also called EMCON.** (JP 3-85)

enemy

A party identified as hostile against which the use of force is authorized. (ADP 3-0)

enclave

A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter. (CNSSI 4009)

essential task

A specified or implied task that must be executed to accomplish the mission. (FM 5-0)

execution

The act of putting a plan into action by applying combat power to accomplish the mission and adjusting operations based on changes in the situation. (ADP 5-0)

friendly force information requirement

Information the commander and staff need to understand the status of friendly force and supporting capabilities. (JP 3-0)

homeland security

A concerted national effort to prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism, major disasters, and other emergencies; and minimize the damage and recover from attacks, major disasters, and other emergencies that occur. (JP 3-27)

hybrid threat

The diverse and dynamic combination of regular forces, irregular forces, terrorists, or criminal elements unified to achieve mutually benefitting effects. (ADP 3-0)

implied task

A task that must be performed to accomplish a specified task or mission but is not stated in the higher headquarters' order. (FM 5-0)

insider threat

A person with placement and access who intentionally causes loss or degradation of resources or capabilities or compromises the ability of an organization to accomplish its mission through espionage, providing support to international terrorism, or the unauthorized release or disclosure of information about the plans and intentions of U.S. military forces. (AR 381-12)

key terrain

An identifiable characteristic whose seizure or retention affords a marked advantage to either combatant. (ADP 3-90)

national special security event

A designated event that, by virtue of its political, economic, social, or religious significance, may be the target of terrorism or other criminal activity. (JP 3-28)

network transport

The processes, equipment, and transmission media that provide connectivity and move data between networking devices and facilities. (FM 6-02)

operational environment

The aggregate of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. (JP 3-0)

operation order

A directive issued by a commander to subordinate commanders for the purpose of effecting the coordinated execution of an operation. **Also called OPORD.** (JP 5-0)

planning

The art and science of understanding a situation, envisioning a desired future, and laying out effective ways of bringing that future about. (ADP 5-0)

preparation

Activities performed by units and Soldiers to improve their ability to execute an operation. (ADP 5.0)

priority intelligence requirement

The intelligence component of commander’s critical information requirements used to focus the employment of limited intelligence assets and resources against competing demands for intelligence support. (JP 2-0)

risk assessment

The identification and assessment of hazards (first two steps of the risk management process). (JP 3-26)

specified task

A task specifically assigned to a unit by its higher headquarters. (FM 5-0)

survivability

All aspects of protecting personnel, weapons, and supplies while simultaneously deceiving the enemy. (JP 3-34)

task-organizing

The act of designing a force, support staff, or sustainment package of specific size and composition to meet a unique task or mission. (ADP 3-0)

technical channels

The chain of authority for ensuring the execution of clearly delineated technical tasks, functions, and capabilities to meet the dynamic requirements of Department of Defense information network operations. (ATP 6-02.71)

threat

Any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland (ADP 3-0).

References

All URLs accessed on 21 January 2025.

REQUIRED PUBLICATIONS

These documents must be available to the intended users of this publication.

Department of Defense Dictionary of Military and Associated Terms. 15 February 2025.

FM 1-02.1. *Operational Terms*. 28 February 2024.

FM 1-02.2. *Military Symbols*. 23 January 2025.

RELATED PUBLICATIONS

These documents are cited in this publication.

CHAIRMAN OF THE JOINT CHIEFS OF STAFF PUBLICATIONS

Chairman of the Joint Chiefs of Staff issuances are available online: https://www.jcs.mil/Library.aspx.

CJCSI 6250.01G. *Department of Defense Satellite Communications*. 26 July 2022.

CJCSM 3320.02E. *Joint Spectrum Interference Resolution (JSIR) Procedures*. 20 May 2022.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS

Most Department of Defense publications are available at the Department of Defense Issuances Website: https://www.esd.whs.mil/Directives/issuances/dodi/.

Most joint publications are available online: https://www.jcs.mil/doctrine.

JP 2-0. *Joint Intelligence*. 26 May 2022.

JP 3-0. *Joint Campaigns and Operations*. 18 June 2022.

JP 3-26. *Joint Combating Terrorism*. 30 July 2020.

JP 3-27. *Joint Homeland Defense*. 12 December 2023.

JP 3-28. *Defense Support of Civil Authorities*. 23 September 2024.

JP 3-29. *Foreign Humanitarian Assistance*. 14 May 2019.

JP 3-34. *Joint Engineer Operations*. 20 February 2025.

JP 3-85. *Joint Electromagnetic Spectrum Operations*. 22 May 2020.

JP 4-09. *Distribution Operations*. 14 March 2019.

JP 5-0. *Joint Planning*. 1 December 2020.

JP 6-0. *Joint Communications*. 4 December 2023.

JP 3-59. *Meteorological and Oceanographic Operations.* 25 November 2024.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: https://armypubs.army.mil.

ADP 3-0. *Operations*. 31 July 2019.

ADP 3-28. *Defense Support of Civil Authorities*. 31 July 2019.

ADP 3-37. *Protection.* 10 January 2024.

ADP 3-90. *Offense and Defense*. 31 July 2019.

ADP 5-0. *The Operations Process*. 31 July 2019.

ADP 6-0. *Mission Command: Command and Control of Army Forces*. 31 July 2019.

ADP 6-22. *Army Leadership and the Profession*. 31 July 2019.

AR 350-1. *Army Training and Leader Development*. 10 December 2017.

AR 381-12. *Threat Awareness and Reporting Program*. 1 June 2016.

AR 525-93. *Army Deployment and Redeployment*. 06 October 2023.

AR 600-8-101. *Personnel Readiness Processing*. 6 March 2018.

ATP 2-01.3. *Intelligence Preparation of the Operational Environment*. 1 March 2019.

ATP 3-12.3. *Electromagnetic Warfare Techniques*. 30 January 2023.

ATP 3-16.02. *Write for Release.* 26 September 2023.

ATP 4-11. *Army Motor Transport Operations.* 14 August 2020.

ATP 4-43. *Petroleum Supply Operations.* 18 April 2022.

ATP 5-19. *Risk Management*. 9 November 2021.

ATP 6-0.5. *Command Post Organization and Operations*. 1 March 2017.

ATP 6-02.2. *Signal Platoon.* 30 December 2020.

ATP 6-02.45. *Techniques for Tactical Signal Support to Theater Operations*. 7 November 2019.

ATP 6-02.53. *Techniques for Tactical Radio Operations*. 13 February 2020.

ATP 6-02.61. *Expeditionary Mission Partner Network Operations.*

06 December 2023

ATP 6-02.70. *Techniques for Spectrum Management Operations*. 16 October 2019.

ATP 6-02.71. *Techniques for Department of Defense Information Network Operations*. 30 April 2019.

ATP 6-02.75. *Techniques for Communications Security*. 18 May 2020.

DA PAM 750-8. *The Army Maintenance Management System (TAMMS) Users Manual*. 22 August 2005.

FM 3-0. *Operations*. 21 March 2025.

FM 3-11. *Chemical, Biological, Radiological, and Nuclear Operations10 April 2025*.

FM 3-12. *Cyberspace Operations and Electromagnetic Warfare*. 24 August 2021.

FM 3-14. *Army Space Operations.* 30 October 2019.

FM 3-96. *Brigade Combat Team*. 19 January 2021.

FM 4-0. *Sustainment Operations*. 14 Augusta 2024.

FM 5-0. *Planning and Orders Production*. 4 November 2024.

FM 6-0. *Commander and Staff Organization and Operations*. 16 May 2022.

FM 6-02. *Signal Support to Operations*. 13 September 2019.

FM 6-27/MCTP 11-10C. *The Commander's Handbook on the Law of Land Warfare*. 7 August 2019.

FM 7-0. *Training*. 14 June 2021.

STP 21-1-SMCT. *Soldier's Manual of Common Tasks, Warrior Skills, Level 1*. 16 October 2023.

STP 21-24-SMCT. *Soldier`s Manual of Common Tasks, Warrior Leader Skill Level 2, 3, And 4*. 9 September 2008.

TB MED 507. *Heat Stress Control and Heat Casualty Management*. 12 April 2022.

TC 6-02.6. (TC 11-6) *Grounding Techniques for Tactical Equipment and Systems*. 22 November 2017.

TC 7-100.2. *Opposing Force Tactics.* 9 December 2011.

TC 7-102. *Operational Environment and Army Learning.* 26 November 2014.

TC 21-305-1. *Training Program for the Heavy Expanded Mobility Tactical Truck (HEMTT), Palletized Load System (PLS), and Load Handling System (LHS) Family of Vehicles.* 19 February 2025.

TC 21-305-2. *Training Program for Night Vision Device Driving Operations*. 17 January 2014.

OTHER PUBLICATIONS

Committee on National Security Systems publications are available online. https://www.cnss.gov/cnss/issuances/Instructions.cfm.

CNSSI 4009. *Committee on National Security Systems (CNSS) Glossary*. 7 March 2022.

WEBSITES

Digital Training Management System Website. https://dtms.army.mil/. (DOD-approved certificate login required.)

Army Training and Certification Tracking System Website. https://atcts.army.mil/iastar/. (DOD-approved certificate login required.)

Army Training Network Website. https://atn.army.mil/. (DOD-approved certificate login required.)

Cyber Lessons and Best Practices Website. https://lwn.army.mil/web/cll/home. (DOD-approved certificate login required.)

Global Combat Support System-Army Website. https://www.gcss.army.mil/Default/. (DOD-approved certificate login required.)

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

Unless otherwise indicated, DA Forms are available on the Army Publishing Directorate Website at https://armypubs.army.mil.

Department of Defense forms are available at: https://www.esd.whs.mil/Directives/forms/.

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

DA Form 5988-E. *Equipment Maintenance and Inspection Worksheet (EGA).*

DD Form 2977. *Deliberate Risk Assessment Worksheet*.

Index

Entries are by paragraph number.

A

access priorities, 3-32

assessment, 3-12

C

civil considerations, 3-127

collective training techniques, 6-5

command and support relationships, 4-56
- assigned, 4-60
- attached, 4-61
- operational control, 4-62
- organic, 4-59
- tactical control, 4-63

command post support, 4-3

command post survivability, 4-6
- command post signatures, 4-18
- dispersion, 4-8
- displacement, 4-10
- redundancy, 4-15
- size, 4-13

communications platoon, 2-51

communications platoon (enroute communications company), 3-45

communications platoon 1, 2-64

communications platoon 2, 2-69

communications security, 3-42

communications-electronics maintenance, 5-37

COMSEC. *See* communications security

congested electromagnetic spectrum, 1-5

contested electromagnetic spectrum, 1-6

corps, 4-34

D

data exfiltration, A-53

defense support of civil authorities, 4-44

denial-of-service, A-44

deployment, 3-18

deployment and employment of units, 3-15

E

electromagnetic signature, limiting, A-4
- camouflage net masking, A-7
- frequent command post displacement, A-11
- line of sight, A-8
- remote antennas, A-9
- satellite site selection and radio frequency Interference, A-13
- terrain masking, A-6

EMCON. *See* emission control

emission control, 4-25

enroute communications company, 2-59
- capabilities, 2-60
- company headquarters, 2-62

execution, 3-11

expeditionary signal battalion, 2-3

expeditionary signal battalion-enhanced, 2-41

expeditionary signal company, 2-8
- capabilities, 2-9
- company headquarters, 2-11

expeditionary signal company-enhanced, 2-45
- capabilities, 2-49
- company headquarters, 2-50

expeditionary signal platoon, 2-15

G

gateway access requests, 3-31

H

heavy signal platoon, 2-30

homeland defense, 4-40

Entries are by paragraph number.

homeland security, 4-42
humanitarian assistance, 4-49
  communications, 4-50
  interoperability, 4-52

I

incident resolution, A-38
information requirements, 3-91

J

joint and area signal company, 2-26
  capabilities, 2-27
  company headquarters, 2-29
joint forcible entry platoon, 3-46

L

life cycle managed systems, 5-6
line of sight communications, 3-38

M

maintenance, 5-1
  below depot, 5-26
  depot, 5-24
  field, 5-10
  maintainer, 5-19
  management, 5-2
  motor and generator, 5-33network, 5-35
  operator and crew, 5-15
  spares management, 5-37
  sustainment, 5-21
  two-level maintenance, 5-8
maintenance requests, 5-31
maintenance support, 5-29
mission analysis, 3-58, 3-64
  enemy, 3-78
mission partner networks, 4-54
mission variables, 3-61

N

non-standard equipment, 5-7

O

obstacles, 3-103
operational environment, 1-1

P

personal electronic devices, A-73
phishing, A-63
plan development at the company level, 3-131
planning, 3-2
positive control, 3-35
pre-combat checks, 3-172
pre-combat inspections, 3-173
pre-deployment, 3-16
preparation, 3-5

R

recovery, 3-175
rehearsal, 3-151
rehearsal methods, 3-164
rehearsal types, 3-157
reporting procedure, A-40
resupply, 5-44
  cache, 5-60
  emergency, 5-56
  routine, 5-47
  service station, 5-53
  service station technique, 5-59
  tailgate, 5-51
  tailgate technique, 5-58
risk assessment, 3-129
roles and responsibilities, 2-70
  company commander, 2-72
  first sergeant, 2-73
  network communication system manager, 2-79
  operations officer, 2-74
  platoon leader, 2-75
  platoon sergeant, 2-77
  satellite communications operations noncommissioned officer, 2-80
  section sergeant, 2-81
  signal operators, 2-83
  team leader, 2-82

S

safety, 6-38
  convoy operations, 6-43
  electrical shock, 6-46
  electromagnetic radiation hazards, 6-39
  fueling and refueling, 6-48
  heat casualties, 6-50
  heavy lifting, 6-42
  tripping, 6-49
SATCOM. *See* satellite communications
satellite access requests, 3-26
satellite communications, 3-22
signal assessment tables, 6-54
social engineering, A-58
social media attacks, A-69
supply, 5-43

Entries are by paragraph number.

support to operations, 4-1
supported units, 3-41

T

tactical communications augmentation, 4-32
tactics, techniques, and procedures, A-1
terrain and weather analysis, 3-95
threat, 1-8
  hybrid, 1-13
  insider, 1-15
  peer, 1-10
threat effects, A-16
  communications jamming, A-19
  jamming, A-17
  joint spectrum interference resolution, A-37
  malicious cyberspace activities, A-43
  positioning, navigation, and timing jamming, A-27
  satellite communications jamming, A-32
time analysis, 3-125
training, 6-1
  combined arms training, 6-11
  digital battle drills, 6-10
  realistic training environment, 6-6
training and evaluation, 6-16
training model, 8-step, 6-20
troop leading procedures, 3-47
tropospheric scatter, 3-40
TTP. *See* tactics, techniques, and procedures

U

unique planning requirements, 3-19
unit organization, 2-1

W

weather, 3-113

This page intentionally left blank.

ATP 6-02.46

07 May 2025

By Order of the Secretary of the Army:

RANDY A. GEORGE
General, United States Army
Chief of Staff

Official:

MARK F. AVERILL
Administrative Assistant
to the Secretary of the Army
2512203

DISTRIBUTION:
Active Army, Army National Guard, and United States Army Reserve. Distributed in electronic media only(EMO).

This page intentionally left blank.

PIN: 220615-001