

---

---

**DEPARTMENT OF DEFENSE INFORMATION  
NETWORK-ARMY PLANNING TECHNIQUES  
NOVEMBER 2021**

---

---

**DISTRIBUTION RESTRICTION:** Approved for public release; distribution is unlimited.

---

---

**Headquarters, Department of the Army**

---

---

This publication is available at Army Publishing Directorate site  
<https://armypubs.army.mil/> and the Central Army Registry site  
<https://atiam.train.army.mil/catalog/dashboard>.

# Department of Defense Information Network- Army Planning Techniques

## Contents

	Page
<b>PREFACE.....</b>	<b>v</b>
<b>INTRODUCTION .....</b>	<b>vii</b>
<b>Chapter 1 PLANNING OVERVIEW .....</b>	<b>1-1</b>
<b>Section I – Operational Environment Overview .....</b>	<b>1-1</b>
Operational Environment.....	1-1
Threats.....	1-2
<b>Section II – Planning Overview .....</b>	<b>1-4</b>
Planning Processes .....	1-4
Operational Environment Considerations.....	1-5
Coordination With Other Staff Elements .....	1-6
<b>Section III – Network Overview .....</b>	<b>1-7</b>
Joint Network.....	1-7
Army Network.....	1-7
Mission Partner Environment .....	1-8
<b>Chapter 2 SIGNAL IN THE MILITARY DECISION-MAKING PROCESS .....</b>	<b>2-1</b>
Signal Staff Estimate .....	2-1
Defining Signal Requirements .....	2-3
Primary, Alternate, Contingency, and Emergency Communications Plan .....	2-4
Paragraph 5 of an Operations Order .....	2-6
Annex H (Signal) .....	2-6
Attachments to Annex H (Signal) .....	2-10
<b>Chapter 3 OTHER PLANNING PROCESSES AND PRODUCTS .....</b>	<b>3-1</b>
<b>Section I – Network Transport and Information Services .....</b>	<b>3-1</b>
Satellite Communications Transport .....	3-1
Satellite Access Requests .....	3-3
Line-of-Sight Transport.....	3-6
Tropospheric Scatter .....	3-6
Combat Net Radios .....	3-7
Link-16.....	3-9
Information Services.....	3-9
Regional Hub Node or Department of Defense Gateway Coordination.....	3-10

	<b>Section II – Networking .....</b>	<b>3-10</b>
	Cybersecurity .....	3-10
	Internet Protocol Planning.....	3-11
	Firewalls .....	3-12
	Quality of Service .....	3-12
	Information Dissemination Management and Content Staging .....	3-12
	<b>Section III – Spectrum Planning .....</b>	<b>3-15</b>
	Frequency Deconfliction .....	3-16
	Frequency Assignment .....	3-16
	Signal Operating Instructions.....	3-17
	Radio Loadsets .....	3-17
	Joint-Tactical Network Operations Toolkit .....	3-18
	Host-Nation Coordination.....	3-18
	<b>Section IV – Communications Security .....</b>	<b>3-18</b>
	Planning Cryptographic Networks.....	3-18
<b>Chapter 4</b>	<b>SIGNAL SITE PLANNING.....</b>	<b>4-1</b>
	<b>Section I – Site Selection .....</b>	<b>4-1</b>
	Signal Site Analysis.....	4-1
	Site Selection .....	4-2
	<b>Section II – Site Planning .....</b>	<b>4-2</b>
	Site Reconnaissance .....	4-2
	Priorities of Work.....	4-3
	Site Security and Defense .....	4-5
	Signature Reduction.....	4-6
<b>Appendix A</b>	<b>ATTACHMENTS TO ANNEX H .....</b>	<b>A-1</b>
<b>Appendix B</b>	<b>EQUIPMENT CUT SHEETS .....</b>	<b>B-1</b>
	<b>GLOSSARY .....</b>	<b>Glossary-1</b>
	<b>REFERENCES.....</b>	<b>References-1</b>
	<b>INDEX .....</b>	<b>Index-1</b>

## Figures

Figure 2-1. Sample Annex H (Signal) format.....	2-6
Figure 2-2. Sample Annex H, Appendix and Tabs .....	2-10
Figure 3-1. Army Centralized Army Service Request System conflict flags .....	3-4
Figure 3-2. Retransmission operations.....	3-8
Figure 4-1. Sample link establishment priorities .....	4-5
Figure A-1. Tab C to Appendix 2–Network node allocation and organization .....	A-3
Figure A-2. Example Tab C to Appendix 3–Voice, video, and data logical network diagram .....	A-6
Figure A-3. Sample Tab E to Appendix 3–Upper tier satellite transmission diagram .....	A-8
Figure A-4. Tab B–Retransmission network diagram .....	A-10
Figure A-5. Sample Tab I–Mission command information systems allocation and interconnections .....	A-11

## Tables

Table 2-1. Signal staff estimate.....	2-3
Table 2-2. Example primary, alternate, contingency, and emergency communications plan by warfighting function .....	2-5
Table 3-1. Network hardening techniques .....	3-15
Table 3-2. Automated Communications Engineering Software signal operating instructions data requirements .....	3-17
Table A-1. Cybersecurity incident battle drill.....	A-2
Table A-2. Voice over internet protocol phone book.....	A-7
Table A-3. Sample Appendix 4–Spectrum management operations emitter list .....	A-12
Table B-1. Example Joint Network Node cut sheet.....	B-2
Table B-2. Tactical flexible multiplexer settings .....	B-3
Table B-3. Sample Command Post Node cut sheet .....	B-4
Table B-4. Sample Tactical Communications Node cut sheet.....	B-5
Table B-5. Sample Point of Presence cut sheet .....	B-6
Table B-6. Sample Satellite Transportable Terminal cut sheet.....	B-8
Table B-7. Sample Phoenix terminal cut sheet .....	B-9

This page intentionally left blank.

## Preface

ATP 6-02.12 provides tactics and techniques for planning signal support and builds on the signal planning information provided in FM 6-02. This publication establishes non-prescriptive ways to perform missions, functions, and tasks associated with planning the secure tactical information network that enables command and control at echelons corps and below.

The principal audience for ATP 6-02.12 is Army Professionals who plan tactical signal support. To apply the planning techniques in this manual, readers should be familiar with ADP 3-0, ADP 5-0, FM 3-0, FM 6-0, and FM 6-02. Commanders and staffs of Army headquarters serving as the joint task force or multinational headquarters should also refer to the 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 ensure that their decisions and actions comply with applicable United States, international, and, in some cases, host-nation laws and regulations. Commanders at all levels will ensure their Soldiers operate in accordance with the law of armed conflict and applicable rules of engagement (see FM 6-27). Commanders also adhere to the Army Ethic as described in ADP 6-22.

ATP 6-02.12 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 6-02.12 applies to the Active Army, Army National Guard or Army National Guard of the United States, and United States Army Reserve, unless otherwise stated.

The proponent for this publication 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 a 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 6-02.12), 506 Chamberlain Avenue, Fort Gordon, GA 30905-5735, or e-mail to [usarmy.gordon.cyber-coe.mbx.gord-fg-doctrine@mail.mil](mailto:usarmy.gordon.cyber-coe.mbx.gord-fg-doctrine@mail.mil).

This page intentionally left blank.



# Introduction

ATP 6-02.12 discusses Army planning processes, the role of signal staffs in the military decision-making process, and the additional planning necessary to integrate tactical signal equipment into the Department of Defense information network-Army. This publication aligns with FM 6-02 while adding additional information on planning for tactical signal support to Army operations at echelons corps and below.

Signal planners must plan signal support according to the fundamental principles of—operational focus, interoperability, agility, trusted systems, shared networks, and network situational awareness.

This publication implements the following American, British, Canadian, Australian, and New Zealand standards: 2105 Edition 4 and 2100 Edition 4.

ATP 6-02.12 contains four chapters and two appendixes:

**Chapter 1** provides an overview of signal planning. Section I discusses the operational environment and threats. Section II provides an overview of planning processes, operational environment considerations, and coordination with other staff elements. Section III discusses the joint and Army network.

**Chapter 2** discusses the role of signal staffs in the military decision-making process. It discusses the signal staff estimate; defining signal requirements; primary, alternate, contingency, and emergency communications planning; paragraph 5 of an operation order; Annex H (Signal) to an operation order; and attachments to Annex H.

**Chapter 3** discusses other planning processes and products. Section I discusses network transport and information services, including satellite communications transport, line-of-sight transport, tropospheric scatter, single-channel radios, signal operating instructions, gateway access, and regional hub node coordination. Section II discusses network planning, including cybersecurity, Internet protocol planning, firewalls, quality of service, unified action partner interoperability, and information dissemination management and content staging. Section III provides an overview of spectrum planning, and section IV discusses communications security.

**Chapter 4** discusses signal site planning. Section I discusses signal site analysis and site selection. Section II discusses site setup, including site reconnaissance, priorities of work, site security and defense, and command post signature reduction.

**Appendix A** provides sample templates for appendixes and tabs to Annex H (Signal).

**Appendix B** provides samples of equipment cut sheets for common signal assemblages.

This page intentionally left blank.

## Chapter 1

# Overview

This chapter provides an overview of signal planning. It starts with a discussion of the operational environment and threats. The chapter introduces planning processes, operational environment considerations, and coordination with other staff elements. This chapter also gives a brief overview of the joint and Army networks.

### SECTION I – OPERATIONAL ENVIRONMENT OVERVIEW

1-1. The experiences of the U.S. Army in Afghanistan and Iraq in the early 21st century are not representative of the most dangerous conflicts the Army will face in the future. While the Army conducted combat operations in both locations, for the most part, it focused its efforts on counterinsurgency operations and stability tasks (FM 3-0). Large-scale combat operations against a peer threat will present much more demanding operational tempo and greater lethality in the future.

## OPERATIONAL ENVIRONMENT

1-2. Factors that affect operations extend far beyond the boundaries of a commander's assigned area of operations. An *area of operations* is an operational area defined by a commander for land and maritime forces that should be large enough to accomplish their missions and protect their forces (JP 3-0). Commanders and their staffs seek to develop and maintain an understanding of their operational environment. An *operational environment* is a composite 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 the air, land, maritime, and space domains, as well as cyberspace and the electromagnetic spectrum.

1-3. Army forces may conduct operations across multiple domains to gain freedom of action for other members of the joint force. The air, land, maritime, space, and cyberspace domains, and their effects on operations are closely interrelated. The complex relationships between the warfighting domains require a cross-domain understanding of the operational environment. Signal leaders must understand the available communications capabilities and interoperability challenges of communications support in each domain. A thorough understanding helps identify opportunities for the command to coordinate with unified action partners and converge effects when operating throughout the multi-domain battlefield.

1-4. Understanding the operational environment is essential for signal leaders, engineers, planners, system operators, spectrum managers, system administrators, and cybersecurity professionals to plan and execute effective signal support. Signal Soldiers must understand signal flow from the end user, through the local area network, through the wide-area network, and the Department of Defense information network-Army (DODIN-A).

## CONGESTED ENVIRONMENT

1-5. Today, all joint force operations depend on assured electromagnetic spectrum access throughout the operational environment (JP 6-0). All forces and supporting agencies depend on the electromagnetic spectrum for communications, information collection, and electromagnetic warfare (EW) capabilities in support of operations in the air, land, maritime, space, and cyberspace domains. Signal systems rely on the electromagnetic spectrum for network transport. For this reason, gaining and maintaining access to the electromagnetic spectrum is critical for signal support to joint and Army operations.

1-6. Within the electromagnetic spectrum, joint forces contend with civil agencies, commercial entities, allied forces, and adversaries for the use of a common electromagnetic spectrum resource (ATP 6-02.70). Competition for the finite available bandwidth results in a congested electromagnetic spectrum, especially when operating in developed nations.

1-7. Signal staffs plan communications and network capabilities to support all anticipated requirements in their operational area. However, in a congested electromagnetic operational environment, there might not be adequate satellite bandwidth and spectrum availability to support all missions. Signal leaders must clearly articulate the limitations and expected level of degradation, so commanders can make appropriate risk decisions and align the available capabilities with their priorities (FM 6-02).

## **CONTESTED ENVIRONMENT**

1-8. Threat cyberspace and EW capabilities jeopardize U.S. freedom of action in cyberspace and the electromagnetic spectrum. Because communications are a key command and control enabler, U.S. military communications and information networks present high-value targets. Peer threats and other adversaries understand the extent of U.S. forces' reliance on communications and automated information systems. Enemies and adversaries are likely to contest U.S. use of cyberspace and the electromagnetic spectrum across the conflict continuum to deny operational access and diminish the effectiveness of U.S. and allied forces.

1-9. A broad array of threat actors challenges the joint force's freedom of action in space, cyberspace, and the electromagnetic spectrum. For example, an enemy that jams positioning, navigation, and timing satellites may render precision fires inaccurate. Signal elements must secure and protect their own systems and be prepared to operate with degraded communications and reduced access to cyberspace and space capabilities.

1-10. Planners must synchronize the scheme of signal support with cyberspace, EW, intelligence, space, and other information-related capabilities to achieve and maintain freedom of action in contested cyberspace and the electromagnetic spectrum while denying the same to adversaries. *Synchronization* is the arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time (JP 2-0). Synchronization of capabilities across multiple domains and warfighting functions maximizes their complementary effects in and through cyberspace and the electromagnetic spectrum.

1-11. While enemy action might cause a degraded environment, degraded capabilities may also occur because of insufficient resources to support all communications requirements. For example, inadequate communications satellite capacity in an operational area may cause congestion and network latency. Jamming or unintentional electromagnetic interference may also cause degradation. The architecture of the tactical network implements redundant communications paths to improve reliability in a degraded environment. Careful signal planning may also mitigate degradation of signal capabilities, whether the degradation occurs naturally or results from hostile actions.

## **THREATS**

1-12. 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 may include individuals, organized or unorganized groups, paramilitary or military forces, nation-states, or national alliances.

1-13. Threats can be broadly categorized as adversaries, enemies, or insiders. 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 (see paragraphs 1-25) present unique challenges because they are trusted individuals with access to Army capabilities and sensitive operational information.

### **Peer Threats**

1-14. Peer threats employ their resources across multiple domains to exploit U.S. vulnerabilities. They use their capabilities to create lethal and nonlethal effects across the operational environment. Peer threats have demonstrated advanced capabilities in long-range precision fires, integrated air defense, and EW. These

threat capabilities demand changes to signal tactics, techniques, and procedures to counter the risks they present.

1-15. Peer threat forces are equally well equipped with the latest technologies as well as the will to use them. Peer threats have capabilities that can directly challenge the United States in all domains. This includes attacks on U.S. satellite communications platforms, links, and terrestrial segments; effects on positioning, navigation, and timing; information warfare and offensive cyberspace operations; and effects in cyberspace and the electromagnetic spectrum designed to deny, disrupt, or exploit U.S. reliance on information systems and networks.

1-16. Peer threats consider U.S. communications, command and control nodes, massed formations, and critical infrastructure key targets during large-scale combat operations. Signal planners should consider positioning radio frequency emitters, such as satellite communications antennas and line-of-sight radio systems, away from major command posts to minimize loss of life. Also, to minimize and command and control capabilities if an enemy targets the communications systems with lethal fires.

## Hybrid Threat

1-17. A *hybrid threat* is the diverse and dynamic combination of regular forces, irregular forces, terrorists, or criminal elements acting in concert to achieve mutually benefitting effects (ADP 3-0). Hybrid threats seek to exploit asymmetric advantages over an adversary to avoid engaging in direct combat.

1-18. Hybrid threats may employ cyberspace attack 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.

## Information Warfare

1-19. Information warfare refers to a threat's use of information activities, such as cyberspace attacks and EW, to gain an information advantage. The threat construct of information warfare merges the disciplines of EW, deception, lethal fires, information protection, perception management, and cyberspace operations into a mutually supporting, integrated capability.

1-20. Adversaries recognize the advantages information warfare activities can provide their tactical commanders. Therefore, they strive to integrate information warfare planning and activities in all tactical missions and battles. Because threat actors integrate their information warfare capabilities, a coordinated and synchronized response is essential. The countermeasures to defend against these capabilities are a combination of signal, cyberspace operations, electromagnetic protection, space, and other information-related capabilities in all domains, along with intelligence and operations security support.

1-21. Signal planners should collaborate closely with cyberspace, EW, space, and intelligence staff when formulating signal support plans to ensure an integrated response to threat information warfare activities. Refer to TC 7-100 for more information about hybrid threats and information warfare.

## INSIDER THREAT

1-22. 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 is not to be confused with operations security or cybersecurity risks, where sensitive operational information may become accidentally compromised and place U.S. operations or personnel at risk.

1-23. Past cases of insider threats have demonstrated that coworkers, associates, friends, and supervisors of those engaging in espionage or terrorist activity commonly overlook potential threat indicators. If these indicators were reported and investigated, they might have minimized the damage to national security or saved the lives of U.S. personnel. Signal planners should maintain awareness of insider threat indicators.

They should also limit access to sensitive operational information to those with a valid clearance and need to know.

## **SECTION II – PLANNING OVERVIEW**

1-24. This section describes the planning process and provides planning considerations for DODIN-A planners. This section also contains options for liaison and collaboration with internal and external staff during the planning process. Visit the Cyber Lessons Learned website for training material, and examples related to signal, cyberspace and EW.

## **PLANNING PROCESSES**

1-25. *Planning* is the art and science of understanding a situation, envisioning a desired future, and determining effective ways to bring that future about (ADP 5-0). Planning helps leaders understand situations; develop solutions to problems; direct, coordinate, and synchronize actions; prioritize efforts, and anticipate events. Signal planners follow the same planning processes as other staff sections.

1-26. Planning requires creative application of doctrine, units, and resources. To plan effective signal support, G-6 and S-6 planners must understand not only signal doctrine but also the fundamentals of maneuver doctrine. If the signal staff does not understand the terms movement to contact or retrograde, they cannot develop plans to support those tactical tasks. Refer to ADP 3-0 for the fundamentals of unified land operations. Refer to ADP 3-90 for the fundamentals of offense and defense.

1-27. DODIN-A planners use network automation planning and management tools to facilitate communications planning, engineering, activation, and modification. Automation tool functions include—

- Create and modify databases for communications system equipment and organizations.
- Define the network topology based on sites and by organizations.
- Create and modify subordinate unit tasks, responsibilities and schedules, and track performance.
- Conduct feasibility analyses using modeling and simulation.
- Create, modify, and support distribution of communications plans and orders communications annexes; joint communications-electronics operating instructions; joint restricted frequency lists; and communications service requests.
- Perform detailed network planning and engineering for a joint force network, including—
  - Circuit switch planning and engineering.
  - Voice network planning and engineering.
  - Data network planning and engineering.
  - Virtual network planning and engineering.
  - Video network planning and engineering.
  - Defense Information Systems Network organizational messaging service planning and engineering.
  - Message switch planning and engineering.
  - Backbone transmission systems planning and engineering across the electromagnetic spectrum, including satellite communications.
  - Radio network planning and engineering.
  - Engineering plans and orders.
  - Coordination for link and network activations/deactivations.
  - Coordination for and integration with host-nation communications system resources into the joint and multinational network.

## MILITARY DECISION-MAKING PROCESS

1-28. The *military decision-making process* is an iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order (ADP 5-0). In simple terms, the military decision-making process is a systematic method to solve a specific military problem.

1-29. The G-6 or S-6 takes an active role throughout the military decision-making process. This ensures the G-6 or S-6 understands the commander's intent and scheme of maneuver and that the scheme of signal support will effectively support the maneuver plan. Refer to FM 6-0 for detailed information about the military decision-making process.

## RAPID DECISION MAKING AND SYNCHRONIZATION PROCESS

1-30. The operational variables of political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT), and mission variables—mission, enemy, terrain, troops, time, civil considerations (METT-TC)—continually change during mission execution. This often invalidates or weakens the chosen course of action. The rapid decision-making and synchronization process allows commanders and staff to adjust the operation order to the current situation.

1-31. The rapid decision-making and synchronization process, based on an existing order and the commander's priorities, is expressed in the order. The rapid decision-making and synchronization process provides a timely and effective solution based on the commander's intent, mission, and concept of operations while avoiding the time-consuming requirements of the military decision-making process. The most important of these control measures is the commander's intent, the concept of operations, and the commander's critical information requirements. The rapid decision-making and synchronization process includes five steps:

- Compare the current situation to the order.
- Determine that a decision, and what type, is required.
- Develop a course of action.
- Refine and validate the course of action.
- Implement the course of action.

## TROOP LEADING PROCEDURES

1-32. Troop leading procedures extend the military decision-making process to the small-unit level. The military decision-making process and troop leading procedures are similar but not identical. They are both linked by the basic Army problem-solving process. Commanders with a coordinating staff use the military decision-making process as their primary planning process. Company-level and smaller units lack formal staff and use troop leading procedures to plan and prepare for operations. This places the responsibility for planning primarily on the commander or small-unit leader (FM 6-0).

## OPERATIONAL ENVIRONMENT CONSIDERATIONS

1-33. War in the emerging operational environment will be fought against adversaries across multiple domains, including the electromagnetic spectrum, and U.S. dominance will not be assured. Adversaries will challenge U.S. force projection via layers of political, military, economic, and cyber standoff and will attempt to divide the Army from its joint and coalition partners. Army forces will have to conduct operations in dense urban areas with complex socio-economic structures (TC 6-02.1).

1-34. Signal support plans must account for the proliferation of threat cyberspace capabilities and their impact on operations as well as operating in a spectrum-congested environment. Threat activities in cyberspace can disrupt friendly information systems and degrade joint command and control. Threat operations in cyberspace are often less encumbered by treaty, law, and policy restrictions than those imposed on U.S. forces. This may allow enemies and adversaries an initial advantage in cyberspace. Signal support elements and staff must maintain an effective cybersecurity program to secure the network against threat activities in cyberspace.

## **COORDINATION WITH OTHER STAFF ELEMENTS**

1-35. In operations, effective command and control requires continuous close coordination, synchronization, and information sharing across staff sections. As a coordinating staff officer, the G-6 or S-6 provides signal subject matter expertise for the commander and other staff elements.

### **OPERATIONS STAFF**

1-36. Signal planners must maintain continual coordination with the G-3 or S-3 staff. The G-3 or S-3 is the chief of the movement and maneuver warfighting function and the principal staff officer responsible for all matters concerning training, operations and plans, and force development and modernization. In addition to coordinating the activities of the movement and maneuver warfighting function, the operations officer is the primary staff officer for integrating and synchronizing the operation as a whole for the commander (FM 6-0).

1-37. The G-3 or S-3 ensures warfighting function integration and synchronization across the planning horizons in current operations integration, future operations, and plans integrating cells. The G-6 or S-6 collaborates closely with the G-3 or S-3 to understand the commander's intent and concept of operations and ensures signal plans adequately support the proposed course of action.

### **INTELLIGENCE STAFF**

1-38. G-6 or S-6 planners need an understanding of the current threat situation and electromagnetic order of battle to plan survivable communications. Continual collaboration with the G-2 or S-2 section throughout planning and operations ensures signal staffs understand the threat situation and can plan and implement appropriate countermeasures.

### **CYBER ELECTROMAGNETIC WARFARE OFFICER**

1-39. EW personnel plan the employment of electromagnetic attack, select frequencies for targeting, analyze the probability of frequency fratricide and collaborate with the G-6 or S-6 to mitigate harmful effects from EW to friendly personnel, equipment, and facilities.

1-40. G-6 or S-6 planners should work closely with the cyber electromagnetic warfare officer to minimize the electromagnetic signature of signal sites. Measures to minimize or mask the command post signature include electromagnetic masking, terrain masking, and camouflage net masking.

1-41. The cyber electromagnetic warfare officer and the G-6 or S-6 consider effects on friendly communications when developing an electromagnetic protection plan. A plan that maximizes electromagnetic protection can overly restrict the friendly use of communications assets. The cyber electromagnetic warfare officer maintains a balance regarding the unit's ability to communicate with the planned level of electromagnetic protection.

1-42. The cyber electromagnetic warfare officer may also plan and execute electromagnetic deception to create ambiguity about the location of friendly command posts and communications sites. Electromagnetic decoys can also mask command post dislocation by making it appear the command post is still operating in the same location. Refer to ATP 3-12.3 for more information about electromagnetic deception and electromagnetic protection.

### **LOGISTICS STAFF**

1-43. Sustainment is critical to sustained operations. The ability of operators and crews to maintain and repair signal systems is limited to replacement of onboard spares. The logistics staff and maintenance support units maintain most spare parts. Supply points and maintenance collection points are essential to mission success and operate throughout the corps and division areas of operations.



## Supply

1-44. Maintenance organizations require repair parts as well as tools and test equipment to execute their field and sustainment maintenance missions. Replenishment of shop stock and bench stock is critical to preserve readiness (ATP 4-33).

## Maintenance

1-45. Each maneuver brigade has an assigned brigade support battalion with a forward support company and a field maintenance company. In the other brigades, the forward support company supports the maneuver battalions. The field maintenance company supports the brigade headquarters and other non-maneuver elements in the brigade.

1-46. In the maneuver battalion, the S-6 works in conjunction with the logistics staff, support operations, communications-electronics maintenance shop, and the forward support company commander to develop a comprehensive maintenance plan. The maintenance plan includes coordination for contractor field service representative support.

1-47. Some units in the brigade have limited or no organic field maintenance capability or capacity. These units normally receive field maintenance support or augmentation from a supporting maintenance organization.

## SECTION III – NETWORK OVERVIEW

1-48. Across the globe, information is increasingly available in near real time. The DODIN-A provides the ability to access this information from anywhere at any time. Access to information enables decision making, leadership, and combat power. It is also key to seize, gain, and retain the initiative and to consolidate gains in the operational environment (FM 6-02).

## JOINT NETWORK

1-49. The *Department of Defense information network* (DODIN) 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). DODIN includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems.

1-50. As the Department of Defense (DOD) portion of cyberspace, the DODIN interacts with, and provides connections to, national and global cyberspace. The DODIN consists of joint capabilities provided by the Defense Information Systems Agency combined with Service-specific capabilities provided by the Army, Navy, Air Force, and Marine Corps.

1-51. The joint force depends on the DODIN to connect strategic, operational, and tactical commanders across the globe. When properly secured, operated, and defended, the network enables the right users to access the right information at the right time, with the right security measures in place. The DODIN shares common configurations across all Services enabling real-time collaboration and synchronization with joint mission partners.

## ARMY NETWORK

1-52. 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). The DODIN-A includes all Army automated information systems and networks, including the stand-alone networks supporting intelligence, sustainment, medical, Army special operations forces, Army National Guard, and United States Army Reserve.

1-53. The tactical internet is the deployed portion of the DODIN-A. The deployed portion of the network is functionally similar to the commercial Internet because the communications infrastructure uses many of the

same technologies. From a network planning and management standpoint, the tactical internet divides into the upper tier and the lower tier.

### **UPPER TIER TACTICAL INTERNET**

1-54. The upper tier tactical internet provides high-throughput networking at-the-halt to corps command posts, and at-the-halt or on-the-move at the division and brigade combat team. The upper tier is an interoperability point for higher echelons, aviation integration, and interoperability with joint, inter-organizational, and multinational partners. Warfighter Information Network-Tactical (WIN-T) and the scalable network node provide the upper tier tactical internet. The WIN-T combat net radio gateway provides a bridge to connect combat net radio voice networks in the lower tier to the upper tier. Refer to ATP 6-02.60 for more information about the upper tier tactical internet.

### **LOWER TIER TACTICAL INTERNET**

1-55. The lower tier tactical internet supports tactical formations down to the team leader. The lower tier consists of single and multiple channel networking radios at battalion, company and platoon echelons. Advanced networking waveforms and the single-channel ground and airborne radio system (SINCGARS) provide voice and data supporting lower tier communications. The primary lower tier waveforms are Soldier Radio Waveform, Tactical Scalable Mobile Ad Hoc Networking, and SINCGARS.

1-56. Mobile applications enable visualization, operator interface with ancillary devices (such as Global Positioning System), targeting data, voice communications, and sensor capabilities. Planning tools used for current radio systems in the lower tier include—

- Joint Automated Communications-Electronics Operating Instruction System and Automated Communications Engineering Software.
- Joint Enterprise Network Manager.
- Tactical Internet Management System.
- Coalition Joint Spectrum Management Planning Tool.
- Systems Planning, Engineering, and Evaluation Device.

---

*Note.* Refer to ATP 6-02.53 for more information about the lower tier tactical internet.

---

### **MISSION PARTNER ENVIRONMENT**

1-57. Joint forces must effectively exchange information among components, U. S. government departments and agencies, multinational partners, foreign governments, and international organizations as a critical element of efforts to defend the nation and execute the national strategy (JP 6-0).

1-58. The mission partner environment communications network is a secret-releasable network enclave and must be capable of securely integrating mission partners' systems using common information technology infrastructure, enterprise services, and architectures. Use of agreed-upon information and data exchange standards and services enables interoperable information exchange. The Defense Information Systems Agency maintains standards for joining, membership, and exiting the mission partner environment.

1-59. Key aspects of mission partner network implementation include liaisons, identification of communications network requirements, multinational communications agreements, U.S. interpreters, and a coherent release and disclosure policy. Refer to DODI 8110.01 for information about implementation of mission partner environment.

1-60. The Army uses commercial coalition equipment to connect to the coalition network over its tactical communications network. Each coalition country has their own unique transport networks that enable connection to the mission partner environment.

1-61. Commercial coalition equipment provides an easy to transport system that enables the Army to send and receive critical situational awareness information with coalition partners and contribute to a trusted, near real-time, common operating picture across the theater of operations. The commercial coalition equipment is

configurable to provide secure tactical access for the coalition or commercial networks to support both civil and military operations.

1-62. American, British, Canadian, Australian, and New Zealand standards provide network planners with additional planning techniques to integrate mission partner networks. The joining, membership, and exiting instructions provide the processes and technical configurations for access to the mission partner network.

1-63. The joining, membership, and exiting instructions provide users with a template for connection of joint services and mission partners in a trusted federated mission network that is consistent and coherent across the DOD. The joining, membership, and exiting instructions may be used as a template to guide establishment of a federation of networks to support any event with a unique security classification level information and data exchange environment shared by all mission partners electing to connect (CJCSI 5128.01).

This page intentionally left blank.

## Chapter 2

# Signal in the Military Decision-Making Process

This chapter discusses the role of signal staffs in the military decision-making process. It discusses the signal staff estimate; definition of signal requirements; primary, alternate, contingency, and emergency communications planning; Paragraph 5 of an operation order; Annex H (Signal) to an operation order; and attachments to Annex H.

### SIGNAL STAFF ESTIMATE

2-1. A *running estimate* is the continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if planned future operations are supportable (ADP 5-0). Commanders and staffs use running estimates throughout the operations process. In their running estimates, the commander and staff continuously consider the effect of new information and update—

- Facts.
- Assumptions.
- Friendly force status.
- Enemy status, activities, and capabilities.
- Civil considerations.
- Conclusions and recommendations.
- Risk and limitations.

2-2. The G-6 or S-6 staff develops and continually updates the signal staff estimate. At a minimum, the staff maintains a running estimate of friendly capabilities while in garrison or when not actively engaged in operations. The signal staff estimate includes all relevant signal information, including a mission analysis chart outlining—

- Signal equipment on-hand.
- Equipment in-use, non-mission capable, and available.
- Capabilities of available communications systems.
- Projected radio retransmission sites.
- Combat net radio coverage.
- Status of communications and automated information systems.
- Projected communications node locations.

2-3. The staff immediately begins updating the running estimate upon receipt of a mission. They continue to build and maintain their running estimate throughout planning, preparation, execution, and assessment.

2-4. The staff estimate outlines the G-6 or S-6 and signal elements' ability to support proposed courses of action. Signal planners evaluate the communications and network requirements for each proposed course of action against the available signal support. Evaluating the available signal support includes considering the capabilities and limitations of available signal systems. If signal elements cannot support a proposed course of action, the running estimate helps identify the shortfall.

### FACTS

2-5. A fact is something known to exist or have happened or a statement that is known to be true. A statement of truth or a statement thought to be true at the time. Facts related to the operational variables PMESII-PT and mission variables METT-TC help staffs develop situational understanding. Facts may be truthful, but not relevant. Planners should list facts that relate directly to a proposed course of action to

minimize distractors in decision making. Facts concerning the operational and mission variables serve as the basis for developing situational understanding during planning. When listing facts, planners are careful they are directly relevant to a COA or help commanders make a decision.

### ASSUMPTIONS

2-6. An *assumption* is a specific supposition of the operational environment that is assumed to be true, in the absence of positive proof, essential for the continuation of planning (JP 5-0). Assumptions address gaps in knowledge that are critical for the planning process to continue. Planners should only include assumptions that add value to the planning process.

2-7. Commanders and staffs continuously question whether their assumptions are valid throughout the planning process. Key points concerning the use of assumptions include—

- Assumptions must be logical, realistic, and considered likely to be true, not based on preconceptions.
- Assumptions are necessary for continued planning. If the assumption does not directly affect the decision at hand, it adds no value to the process and increases the chance of an invalid decision.
- Too many assumptions result in a higher probability that the plan or proposed solution may be invalid.
- The use of assumptions requires the staff to develop branches to execute if one or more key assumptions prove false.
- Often, an unstated assumption may prove more dangerous than a stated assumption proven wrong.
- Planners should replace assumptions with the relevant facts, as they become known.

### FRIENDLY FORCE STATUS

2-8. Friendly force status includes location, activity, and combat power of subordinate units from two levels down. The primary focus of the signal staff estimate should be the status and availability of communications equipment and systems to support operations.

### ENEMY ACTIVITIES AND CAPABILITIES

2-9. The running estimate includes enemy status in the area of operations, including composition, disposition, and strength. The G-6 or S-6 should coordinate with the G-2 or S-2 and cyber electromagnetic warfare officer for an accurate assessment of the enemy's cyberspace and EW capabilities, their potential effects on friendly communications, and preventive measures to protect friendly communications capabilities.

### CIVIL CONSIDERATIONS

2-10. The G-2 or S-2 gathers and analyzes information on civil considerations in the area of operations during intelligence preparation of the battlefield. The G-6 or S-6 should include civil considerations that affect signal support in their running estimate.

### CONCLUSIONS AND RECOMMENDATIONS

2-11. During planning, commanders use recommendations from running estimates to select valid (feasible, acceptable, suitable, distinguishable, and complete) courses of action for further analysis. The staff adjusts the running estimate based on course of action development and war gaming. After course of action approval, the signal running estimate forms the basis for Annex H (Signal) of the operation plan or order. During preparation and execution, commanders use recommendations from running estimates to enhance further decision making. See table 2-1 on page 2-3.

Table 2-1. Signal staff estimate

S-6 Running Estimate	
<b>FACTS</b> <ul style="list-style-type: none"> <li>Limited single channel tactical satellite.</li> </ul>	<b>Assumptions</b> <ul style="list-style-type: none"> <li>Frequency modulation with OE-254 and power amplifier will be 35 kilometers.</li> </ul>
<b>Task</b> <ul style="list-style-type: none"> <li>Develop enclave support for communications architecture.</li> <li>Establish retransmission quick response team.</li> <li>Plan communication for follow on operations.</li> </ul>	
<b>Limitations</b> <ul style="list-style-type: none"> <li>Line of sight communications in urban environment.</li> <li>Limited single channel tactical satellite.</li> </ul> <b>Assets available</b> <ul style="list-style-type: none"> <li>Slant report for key mission command systems.</li> </ul> <b>Issues remaining</b> <ul style="list-style-type: none"> <li>Requirements for division networks</li> <li>Wideband satellite segment for command and control mission approval.</li> </ul>	

## DEFINING SIGNAL REQUIREMENTS

2-12. To tailor a signal support package to a particular mission or course of action, the G-6 or S-6 staff accurately identifies and defines signal requirements. This is especially important when packaging an early entry element, a partial deployment, or when tasked to perform a mission beyond the unit's organic capabilities.

2-13. To define signal requirements, the staff should analyze the mission according to planning guidance, existing plans and orders, or a proposed course of action. The staff evaluates—

- The network's purpose.
- The period services are required.
- The elements that need to exchange information.
- The geographic area the network will cover.
- Information exchange requirements.
- Data throughput requirements.
- Types and number of communication systems available to provide signal support.

2-14. The staff identifies signal requirements based on the operational capability required to accomplish the mission, not by a particular unit or communications assemblage. Accurately defining requirements simplifies the process of validation and helps the chain of command source the capability when requesting augmentation. In coordination with the G-2 or S-2 and G-3 or S-3, the G-6 or S-6 determines—

- Services required by type and quantity—
  - Non-classified Internet Protocol Router Network (NIPRNET).
  - SECRET Internet Protocol Router Network (SIPRNET).
  - Joint Worldwide Intelligence Communications System.
  - Secure and non-secure voice.
  - Video teleconferencing.
  - Single-channel radios.
  - Single-channel radio retransmission.

- Coalition—mission partner environment.
- Commercial services.
- Mission and purpose for each service.
- Period of services—
  - Starting date-time group.
  - Ending date-time group, if known.
- Location of services.

## PRIMARY, ALTERNATE, CONTINGENCY, AND EMERGENCY COMMUNICATIONS PLAN

2-15. Communications systems enable commanders to accomplish the mission by connecting them with higher, subordinate, supporting, and supported elements during changing and uncertain conditions. Recognizing that military operations are volatile, uncertain, complex, and ambiguous, the Army has long practiced a primary, alternate, contingency, and emergency (PACE) methodology for use in communications planning.

2-16. A PACE communications plan provides predictability and redundancy to communications systems in degraded, contested, or congested environments. Building an effective PACE plan may be simultaneously the most useful and challenging practice for communications planners. The key to a good PACE plan is to establish system and network redundancy, so some means of communication is always available.

2-17. Signal leaders and planners must understand their organization's authorized and available communications capabilities and limitations, as well as the personnel and logistical requirements to employ and sustain the capabilities. Commanders and leaders should develop this understanding through action by employing all of their organic equipment during unit training, correcting deficiencies through unit training, and maintenance and supply programs.

2-18. During the military decision-making process, G-6 or S-6 planners consider the effects of the operational environment, the scheme of maneuver, and other warfighting function tasks. Planners allocate communications capabilities to each level of the PACE plan, ensuring the proposed plan is feasible, acceptable, suitable, distinguishable, and complete.

- **Feasible.** The unit and subordinates must have enough working systems to implement each step of the PACE plan.
- **Acceptable.** Time needed to set up a redundant capability must not interfere with the unit's operation or a command post displacement.
- **Suitable.** Redundant capabilities must have the capacity to meet the commander's requirements.
- **Distinguishable.** Redundant communications means cannot rely on a denied method. For example, if network data were not available, Voice over Internet Protocol would be a poor backup method. If very high frequency (VHF) radio communications become degraded or denied, the next step in the PACE plan should use a different transmission medium.
- **Complete.** The scheme of signal support should outline each means of communication, along with triggers for execution.

2-19. The PACE plan should be as simple as possible to support reliable communications during fast-paced operations. If possible, PACE plans should revolve around warfighting functions. The principal warfighting functions for the purposes of PACE planning are movement and maneuver, intelligence, fires, and sustainment. The G-6 or S-6 does not dictate PACE plans for these warfighting functions but does educate the warfighting function leads on available capabilities during operations and assists the warfighting function staff in formulating a PACE plan (ATP 6-0.5).

2-20. Planners should identify appropriate PACE systems for each phase—for example, defense, offense, or consolidation of gains—and publish them in Annex H (Signal) of the operation order. An emergency means of communication does not necessarily have to be equipment; it may be a procedure such as moving back to the last known effective communications point or rallying at a specified grid coordinate. The PACE plan



helps ensure communications availability if the primary means of communication fails. Table 2-2 shows an example of a simple PACE plan for one phase of an operation, aligned with warfighting functions.

**Table 2-2. Example primary, alternate, contingency, and emergency communications plan by warfighting function**

	<i><b>Movement and Maneuver</b></i>	<i><b>Intelligence</b></i>	<i><b>Fires</b></i>	<i><b>Sustainment</b></i>
Primary	VHF (CMD net)	VHF (O&I)	AFATDS	VHF (A&L)
Alternate	TACSAT	JBCP	VHF (voice)	JBCP
Contingency	JBCP	TACSAT (voice)	VHF (digital)	TACSAT (voice)
Emergency	HF (chat)	TIGR	JBCP	HF (chat)
<b>Legend:</b>				
AFATDS	Advanced Field Artillery Tactical Data System	JBCP	Joint Battle Command Platform	
A&L	administrative and logistics	O&I	operations and intelligence	
CMD	Command	TACSAT	tactical satellite	
FM	frequency modulation	TIGR	tactical ground reporting	
HF	high frequency	VHF	very high frequency	

## PARAGRAPH 5 OF AN OPERATIONS ORDER

2-21. The G-6 or S-6 usually prepares Paragraph 5 (Command and Signal) of the base plan or order in coordination with the G-3 or S-3. The G-6 or S-6 lists task-organized units in the appropriate annexes. Refer to FM 6-0 for the template for Paragraph 5 of an operations plan or order.

## ANNEX H (SIGNAL)

2-22. Commanders and their staffs use Annex H (Signal) to describe how signal elements support the concept of operations described in the base plan or order. The G-6 or S-6 develops Annex H (Signal) using the five-paragraph attachment format. See figure 2-2, pages 2-6 through 2-9.

<b>[CLASSIFICATION]</b> <i>Place the classification at the top and bottom of every page of the attachments. Place the classification marking at the front of each paragraph and subparagraph in parentheses. Refer to AR 380-5 for classification and release marking instructions.</i>
<b>Copy ## of ## copies</b> <b>Issuing headquarters</b> <b>Place of issue</b> <b>Date-time group of signature</b> <b>Message reference number</b>
<i>Include the full heading if attachment is distributed separately from the base order or higher-level attachment.</i>
<b>ANNEX H (SIGNAL) TO OPERATION PLAN/ORDER [number] [(code name)]—[issuing headquarters] [(classification of title)]</b>
<b>(U) References:</b> <i>List documents essential to understanding the annex.</i>
<i>a. List maps and charts first. Map entries include series number, country, sheet names or numbers, edition, and scale.</i>
<i>b. List other references in subparagraphs labeled as shown.</i>
<i>c. Doctrinal references for signal support include FM 5-0, FM 6-02, ATP 6-02.45, ATP 6-02.53, ATP 6-02.54, ATP 6-02.60, ATP 6-02.70, ATP 6-02.71, and ATP 6-02.75.</i>
<b>(U) Time Zone Used throughout the Order:</b> <i>Write the time zone established in the base plan or order.</i>
<b>(U) Task Organization:</b> <i>Describe the organization of forces (to include attachments and detachments) to/from the issuing headquarters and their command and support relationships. State when each attachment or detachment is effective (for example, on order, on commitment of the reserve). Refer to Annex A (Task Organization) if long or complicated.</i>

**Figure 2-1. Sample Annex H (Signal) format**

[CLASSIFICATION]
<p><b>ANNEX H (SIGNAL) TO OPERATION PLAN/ORDER [number] [(code name)]—[issuing headquarters] [(classification of title)]</b></p> <p>1. (U) Situation. <i>Include information affecting signal support that paragraph 1 of the operation plan or operation does not cover, or that needs expansion.</i></p> <p>a. (U) Area of Interest. <i>Describe the area of interest, which includes the area of influence in all five domains and the electromagnetic spectrum as it relates to signal support. Refer to Annex B (Intelligence) as required. This is an opportunity to define the cyber area of interest, which does not always align with the physical area of interest, and is arguably much larger. Include key concentration points of network (regional hub node, regional cyber center, joint regional security stack locations, and tactical hub node placement, if outside the area of operations).</i></p> <p>b. (U) Area of Operations. <i>Describe the area of operations as it relates to signal support. Refer to Appendix 2 (Operation Overlay) to Annex C (Operations).</i></p> <p>(1) (U) Terrain. <i>Describe the aspects of physical and logical terrain (including key terrain in cyberspace and the electromagnetic spectrum) that impact signal support. Refer to Annex B (Intelligence) and Appendix 12 (Cyberspace Electromagnetic Activities) to Annex C (Operations) as required.</i></p> <p>(2) (U) Weather. <i>Describe all critical weather aspects that impact signal support such as precipitation, wind, and solar weather that also may impact network availability or reliability in the area of operations. Refer to Annex B (Intelligence) as required.</i></p> <p>c. (U) Enemy Forces. <i>List known and templated locations and activities of enemy communications, cyber, and electromagnetic warfare units that may influence the area of operations or area of interest. List enemy capabilities (including cyber and electromagnetic warfare) that impact signal support. State expected enemy courses of action that may impact friendly ability to communicate. Refer to Annex B (Intelligence) as required.</i></p> <p>d. (U) Friendly Forces. <i>Briefly identify the signal mission of friendly forces and the objectives, goals, and missions of civilian organizations that impact support. Refer to Annex A (Task Organization) and Annex C (Operations) as required.</i></p> <p>(1) (U) <u>Higher Headquarters Two Levels Up</u>. <i>Identify the higher headquarters mission and commander's intent two echelons above.</i></p> <p>(2) (U) <u>Higher Headquarters One Level Up</u>. <i>Identify the higher headquarters mission, commander's intent, and concept of operations one echelon above.</i></p> <p>(3) (U) <u>Missions of Adjacent Units</u>. <i>Identify and state the missions of adjacent units and other units whose actions have a significant impact on the issuing headquarters.</i></p> <p>(4) (U) <u>Signal Support Impact of Adjacent Units</u>. <i>Identify and state the missions of adjacent units and other units whose actions have a significant impact on the issuing headquarters' signal support.</i></p> <p>e. (U) <u>Interagency, Intergovernmental, and Nongovernmental Organizations</u>. <i>Identify and state the objectives or goals of those non-Department of Defense organizations that have a significant role within the area of operations. Refer to Annex V (Interorganizational-Interagency Coordination) as required.</i></p>
[page number] [CLASSIFICATION]

Figure 2-1. Sample Annex H (Signal) format (continued)

[CLASSIFICATION]
<p><b>ANNEX H (SIGNAL) TO OPERATION PLAN/ORDER [number] [(code name)]—[issuing headquarters] [(classification of title)]</b></p> <p>f. (U) <u>Risk</u>. <i>State the risk to mission, risk to network, and risk to personnel if the concept of signal support is not followed or supported. Identify entry points into cyberspace, which are higher vulnerability areas, such as physical nodes connected to commercial networks and virtual local area network traffic.</i></p> <p>2. (U) <b>Mission</b>. <i>Support [State the mission of the functional area in support of the base plan or order].</i></p> <p>3. (U) <b>Execution</b>.</p> <p>a. (U) <u>Concept of Signal Support</u>. <i>Describe how signal elements support the commander's intent and concept of operations, by phase, as described in the base plan or order. Describe the templated locations of all command and control nodes including command posts and retransmission sites needed to support the concept of operations. Describe the systems and capabilities residing at each of the command posts to enable primary, alternate, contingency, and emergency communication to higher, subordinate, and adjacent units as required. Define the primary, alternate, contingency, and emergency communication plan as it is nested within the concept of signal support. Define triggers to transition command and control and technical channels across the various command posts throughout the operation. Establish the priorities of support to units for each phase of the operation. Refer to Annex C (Operations) as required.</i></p> <p>(1) <u>Scheme of Department of Defense Information Network Operations</u>. <i>Describe how Department of Defense information network operations (including cybersecurity and communications security) support each phase of the operation in the base plan or order</i></p> <p>(2) <u>Scheme of Network Transport and Information Services</u>. <i>Describe how network transport systems (satellite, line of sight, radio, radio retransmission, cable, and wire) and information services support each phase of the operation in the base plan or order.</i></p> <p>(3) <u>Scheme of Spectrum Management Operations</u>. <i>Describe how spectrum management and frequency deconfliction support each phase of the operation in the base plan or order.</i></p> <p>b. (U) <u>Tasks to Subordinate Units</u>. <i>Further description of tasks nested in the base order. List signal support tasks assigned to subordinate signal units not contained in the base order. Each task must include who (the subordinate unit assigned the task), what (the task itself), when, where, and why (purpose). Include tasks for supporting interagency, intergovernmental, and nongovernmental organizations. Use a separate subparagraph for each unit. List units in task organization sequence. Place tasks that affect two or more units in paragraph 3c (Coordinating Instructions).</i></p> <p>c. (U) <u>Tasks to Staff</u>. <i>Include specific staff tasks, which must be completed in order to execute the mission. This could include account validation or creation requirements, computer imaging tasks, nomination of guard and taboo frequencies, mission command validation exercise requirements, or other key events officer requires authentication and only the last name and rank of the commander appear in the signature block.</i></p> <p style="text-align: center;">[page number] [CLASSIFICATION]</p>

Figure 2-1. Sample Annex H (Signal) format (continued)

<p style="text-align: center;"><b>[CLASSIFICATION]</b></p> <p><b>ANNEX H (SIGNAL) TO OPERATION PLAN/ORDER</b> [number] [(code name)]—[issuing headquarters] [(classification of title)]</p> <p>d. (U) <u>Coordinating Instructions</u>. List only instructions applicable to two or more subordinate units not covered in the base plan or order such as timelines for communications exercises, command and control validation exercises, and communications specific rehearsals.</p> <p><b>4. (U) Sustainment.</b> Identify priorities of sustainment for key signal support capabilities and specify additional instructions as required in the paragraph below. Refer to Annex F (Sustainment) as required.</p> <p>a. (U) <u>Logistics</u>. Use subparagraphs to identify priorities and specific instructions for signal logistics support by phase and by communications site. Refer to Annex F (Sustainment) and Annex P (Host-Nation Support) as required.</p> <p>b. (U) <u>Personnel</u>. Define plan for rotating personnel through communications sites.</p> <p>c. (U) <u>Health Service Support</u>. Refer to Annex F (Sustainment) as required.</p> <p>d. (U) <u>Financial Management</u>. Refer to Annex F (Sustainment) as required.</p> <p>e. (U) <u>Maintenance Plan</u>. Describe field service representative support plan, maintenance evacuation plan, resourcing plan for non-mission capable items, locations of unit spares for critical communications systems, scheduled network outages, and authorized service interruptions.</p> <p><b>5. (U) Command and Signal.</b></p> <p>a. (U) <u>Command</u>.</p> <p>(1) (U) <u>Location of Key Signal Leaders</u>. State the locations of the G-6 (S-6) and key signal unit commanders and staff officers during each phase of the operation.</p> <p>(2) (U) <u>Succession of Technical Control</u>. State the succession of technical control authority, if not covered in the unit's standard operating procedures.</p> <p>(3) (U). <u>Command Posts</u>. Describe the employment of command posts (CPs), including the location of each CP and its time of opening and closing, as appropriate. State the primary controlling CP for specific tasks or phases of the operation (for example, "The division tactical command post will control the air assault").</p> <p>b. (U) <u>Signal</u>. Describe the concept of signal support, including location and movement of key signal nodes and critical electromagnetic spectrum considerations throughout the operation. State the primary, alternate, contingency, and emergency (PACE) communications plan. Refer to Annex H (Signal) as required.</p> <p><b>ACKNOWLEDGE:</b> Include only if attachment is distributed separately from the base order.</p> <p style="text-align: right;">[Commander's last name] [Commander's rank]</p> <p>The commander or authorized representative signs the original copy of the attachment. If the representative signs the original, add the phrase "For the Commander." The signed copy is the historical copy and remains in the headquarters' files.</p> <p><b>OFFICIAL:</b></p> <p>[Authenticator's name] [Authenticator's position]</p> <p>Use only if the commander does not sign the original attachment. If the commander signs the original, no further authentication is required. If the commander does not sign, the signature of the preparing staff officer requires authentication and only the last name and rank of the commander appear in the signature block.</p> <p><b>ATTACHMENTS:</b> List lower-level attachment (appendixes, tabs, and exhibits). If a particular attachment is not used, place "not used" beside the attachment number. Unit SOPs will dictate attachment development and format. Common attachments include the following:</p> <p style="text-align: center;">[page number] <b>[CLASSIFICATION]</b></p>
--

Figure 2-1. Sample Annex H (Signal) format (continued)

## ATTACHMENTS TO ANNEX H (SIGNAL)

2-23. Appendixes and their associated tabs provide additional information required to implement the scheme of signal support detailed in Annex H. The format and content for appendixes and tabs follow unit standard operating procedures. Appendixes and suggested tabs to Annex H are found in figure 2-3.

[CLASSIFICATION]
<p><b>ANNEX H (SIGNAL) TO OPERATION PLAN/ORDER [number] [(code name)]—[issuing headquarters] [(classification of title)]</b></p> <ul style="list-style-type: none"> <li>● Appendix 1 – Concept of Signal Support Overlay. <ul style="list-style-type: none"> <li>▪ Tab A – Retransmission Team Mission Checklist.</li> </ul> </li> <li>● Appendix 2- Department of Defense Information Network Operations. <ul style="list-style-type: none"> <li>▪ Tab A – Cybersecurity Incident Battle Drill.</li> <li>▪ Tab B – Cybersecurity Incident Report.</li> <li>▪ Tab C – Network Node Allocation and Organization.</li> <li>▪ Tab D – Network Outage Procedures and Report.</li> <li>▪ Tab E – Scheme of Network Monitoring.</li> </ul> </li> <li>● Appendix 3 – Network Transport and Information Services. <ul style="list-style-type: none"> <li>▪ Tab A – Line-of-Sight Analysis.</li> <li>▪ Tab B – High Frequency Radio Network Diagram.</li> <li>▪ Tab C – Voice, Video, Data Logical Network Diagrams.</li> <li>▪ Tab D – Voice over Internet Protocol Phonebook.</li> <li>▪ Tab E – Upper Tier Satellite Transmission Diagram.</li> <li>▪ Tab F – Coalition Forces Network Diagram and Foreign Disclosure Guidance.</li> <li>▪ Tab G – Satellite Access Authorizations and Gateway Access Authorizations.</li> <li>▪ Tab H – Retransmission Network Diagram.</li> <li>▪ Tab I – Mission Command Information Systems Allocation and Interconnections (Battle Command Common Server/tactical server infrastructure configurations).</li> <li>▪ Tab J – Tactical Satellite Network Diagram.</li> <li>▪ Tab K – Digital Fires Diagram.</li> </ul> </li> <li>● Appendix 4 – Spectrum Management Operations. <ul style="list-style-type: none"> <li>▪ Tab A – Signal Operating Instructions and Frequency Allocation (Commo Card; Tactical Radios).</li> <li>▪ Tab B – Signal Operating Instructions (Lightweight Directory Access Protocol Data Interchange Format).</li> <li>▪ Tab C – Joint Restricted Frequency List.</li> <li>▪ Tab D – Joint Spectrum Interference Resolution Report Format and Procedures.</li> <li>▪ Tab E – Guarded Frequency List.</li> </ul> </li> <li>● Appendix 5 – Communications Security. <ul style="list-style-type: none"> <li>▪ Tab A – Communications Security Callout Message.</li> <li>▪ Tab B – Known Supersession Dates.</li> <li>▪ Tab C – Communications Security Compromise Procedures.</li> </ul> </li> </ul> <p><b>DISTRIBUTION:</b> <i>Show only if distributed separately from the base order or higher-level attachments.</i></p> <p style="text-align: center;">[page number] [CLASSIFICATION]</p>

**Figure 2-2. Sample Annex H, Appendix and Tabs**

2-24. Units can modify these attachments to meet their specific needs, or create additional attachments as necessary. See appendix A for example templates for the recommended appendixes and tabs to Annex H (Signal).

This page intentionally left blank.



## Chapter 3

# Other Planning Processes and Products

This chapter discusses various planning processes and planning products. Section I discusses network transport and information services, including satellite communications transport, line-of-sight transport, tropospheric scatter, single-channel radios, signal operating instructions, gateway access, and regional hub node coordination. Section II discusses network planning, including cybersecurity, Internet protocol planning, firewalls, quality of service, unified action partner interoperability, and information dissemination management and content staging. Section III discusses spectrum planning to include spectrum management operations. Section IV provides information on planning cryptographic networks and communications security.

### SECTION I – NETWORK TRANSPORT AND INFORMATION SERVICES

- 3-1. *Network transport* is the processes, equipment, and transmission media that provide connectivity and move data between networking devices and facilities (FM 6-02). Network transport connects elements across all echelons, so the DODIN-A can operate as an integrated network. Signal staffs plan redundant means of network transport for reliability and survivability in contested operational environments. Key network transport means for planning include satellite communications, line of sight, tropospheric scatter, and single-channel radio systems.
- 3-2. Information services allow access, storage, and sharing of information among mission partners, as well as dynamically tailoring and prioritizing information to support the mission and affect the operational environment. Deployed forces access Defense Information Systems Network services through satellite communications reachback to the regional hub node or DOD gateway.

### SATELLITE COMMUNICATIONS TRANSPORT

- 3-3. Satellite communications provide significant advantages for an expeditionary force. Connecting the tactical network to the sustaining base via satellite communications transport provides full access to Defense Information Systems Network services as soon as the first nodes establish the network, even in remote operational environments.
- 3-4. Army satellite communications planners should be familiar with—
- The Satellite Communications Database.
  - Requirements submission.
  - Operation in degraded and denied environments.
  - Satellite access requests.
  - Gateway access requests.
  - Satellite communications access priorities.
  - Satellite communications apportionment.
  - Access planning.
  - Redundant communications procedures.
  - Allocation process.
  - After action reporting.
  - Planner checklist.

3-5. The satellite communications database is a consolidated repository of all validated military satellite communications requirements. Planners must ensure a validated satellite database number associated with a specific mission requirement is provided on a satellite access request. For more information on the satellite communications database refer to CJCSI 6250.01F.

3-6. Satellite communications planning must take place as early as possible in the planning process to allow sufficient time for the chain of command, regional satellite communications support center, and the Defense Information Systems Agency to review and approve satellite access requests and gateway access requests.

## **WIDEBAND SATELLITE COMMUNICATIONS**

3-7. The Army wideband satellite communications architecture largely provides range extension for the Army common user voice and data systems. Wideband satellite communications extends switched and network subscriber services to deployed forces. It provides reachback to the DODIN for sustaining base support, operational information, and Defense Information Systems Network services. Wideband satellite communications provides the global connectivity needed to support Army operations. Wideband systems operate across the super high frequency spectrum of 3 to 30 GHz range, including the C, Ku, K, Ka, S, and X radio frequency bands. (See ATP 6-02.54 for information on Army satellite planning techniques).

### **Frequency Division Multiple Access**

3-8. Frequency division multiple access dedicates a frequency and a block of bandwidth to a single satellite communications link. Corps, division, and brigade headquarters use frequency division multiple access links to meet their relatively high data throughput requirements for reachback to the sustaining base. Planners submit satellite access requests for frequency division multiple access for—

- Tactical hub node, if used.
- Satellite transportable terminal associated with the tactical communications node at division and brigade combat team.
- Satellite transportable terminal associated with the joint network node at corps and multifunctional support brigade.
- Phoenix terminal.

### **Time Division Multiple Access (Network Centric Waveform)**

3-9. With network centric waveform, many terminals share a given frequency and bandwidth block in time slots. Network centric waveform allocates limited satellite bandwidth more efficiently than frequency division multiple access, at the cost of relatively lower throughput. Planners submit network centric waveform satellite access requests for—

- Tactical hub node, if used.
- Tactical communications nodes at division, brigade, and battalion.
- Satellite transportable terminal associated with the tactical communications nodes at division, brigade and battalion.
- Satellite transportable terminal associated with the joint network node at corps and multifunctional support brigade.
- Satellite transportable terminal associated with the command post node at battalion headquarters.
- Point of Presence at the division, brigade, and battalion.
- Soldier Network Extension.

## **GLOBAL AGILE INTEGRATED TRANSPORT**

3-10. The Global Agile Integrated Transport system allows commanders to maintain situational awareness from garrison to deploy elements through the regional hub node. The global agile integrated transport system enables access to the tactical DODIN-A enclave. Planners request access to the global agile integrated transport system using the satellite access request. Elements connect to the system through the installation's network enterprise center.

## SATELLITE ACCESS REQUESTS

3-11. Planners submit satellite access requests through either the Army Centralized Army Service Request System or Joint Integrated Satellite Communications Tool. The network engineer identifies the mission requirements and terminals to use, and the spectrum manager completes the satellite access request.

3-12. The engineer determines—

- Mission starting and ending date-time group.
- Mission priority.
- Type of satellite—commercial or military.
- Terminals used—listed by satellite database number.
- Modulation type—frequency division multiple access, time division multiple access, network centric waveform.
- Type of services required—voice, data, or voice and data.
- Data throughput required.
- Point of contact information for each terminal to establish positive control.
- Geographic location of each terminal—latitude and longitude.

3-13. Some WIN-T node types can support frequency division multiple access and time division multiple access simultaneously. This requires planners to complete a full satellite access request for each modulation type requested.




## GATEWAY ACCESS REQUEST

3-14. Gateway access request submission is similar to the satellite access request. Planners submit a gateway access request for access to Defense Information Systems Network services. The Defense Information Systems Agency is the controlling organization for gateway access request approvals. The network engineer defines the service requirements and the spectrum manager submits the gateway access request using the Joint Integrated Satellite Communications Tool over SIPRNET. The request routes through the chain of command to the theater Army headquarters for validation. The theater Army routes the validated gateway access request to the regional satellite communications support center and the Defense Information Systems Agency. Upon approval, the Defense Information Systems Agency generates a gateway access authorization and returns it to the requesting unit and the servicing DOD gateway facility.

## ARMY CENTRALIZED ARMY SERVICE REQUEST SYSTEM

3-15. Network planners submit satellite communications access requests for commercial satellite allocations using the Army Centralized Army Request System (ACAS). The ACAS is a web based platform and database. The ACAS consolidates the Army satellite communications service request processes (worldwide) and provides centralized Army satellite communications service request processing through a web browser interface. The ACAS is the standard application used to request and generate commercial satellite access requests and all Army satellite communications service requests for satellite communications bandwidth authorization and connections to the network service center training and regional hub nodes. Planners should register for ACAS and adhere to the submission timelines provided on the ACAS website. Please see the reference page for the ACAS website.

3-16. Registered ACAS planners adhere to and take action for conflicts related to mission requests. Conflicts include missions that occur during authorized service interruptions, missions with overlapping time frames, or a mission terminal with a validated overlapping time frame. Please see the reference page for the ACAS website. Figure 3-1 provides icon examples of conflict flags. This graphic should be seen in color for complete clarity.

	<b>The cone indicates this mission conflicts with an authorized service interruption.</b>
	<b>The red flag indicates a terminal in this mission is also in other missions with an overlapping time frame.</b>
	<b>The blue flag indicates acknowledged and validated reason for a conflict for a mission terminal with an overlapping time frame.</b>

**Figure 3-1. Army Centralized Army Service Request System conflict flags**

### **JOINT INTEGRATED SATELLITE COMMUNICATIONS TOOL**

3-17. The Joint Integrated Satellite Communications Tool application automates the satellite access request and satellite access authorization processes by providing a user request platform that routes coordination activities. This produces the authorized satellite access document. The Joint Integrated Satellite Communications Tool uses authoritative satellite configuration data, significant network, terminal, and mission related data from the joint satellite mission planning system.

3-18. Satellite communications planners draft and submit satellite access requests through approval chains to the combatant command to validate the request against combatant command missions. Once validated, the regional satellite communications support center plans the validated request for satellite communications services against available resources, provides a technical solution, and implements the request in whole or part and documents within a satellite access authorization. The Joint Integrated Satellite Communications Tool collects the required satellite access request and satellite access authorization information throughout the process and provides a platform for the coordination, approval, and execution of approved satellite access. See reference page for the Joint Integrated Satellite Communications Tool Website.

### **COMMERCIAL SATELLITE COMMUNICATIONS**

3-19. If available military satellite resources are not adequate to support operations, the DOD can use commercial satellite communications providers to provide the additional bandwidth needed. The Army employs a disciplined process of mission analysis, solution analysis, and resource analysis to obtain commercial satellite services. The network technician and spectrum manager submit an Army service request for commercial satellite access using the ACAS over NIPRNET. Refer to ATP 6-02.54 for more information about commercial satellite communications.

### **PROTECTED SATELLITE COMMUNICATIONS (EXTREMELY HIGH FREQUENCY)**

3-20. When operating in a contested environment, conventional military communications, including satellite communications, are subject to disruption by enemy electromagnetic attack. Corps, division, and brigade headquarters can use the Secure Mobile Anti-Jam Reliable Tactical Terminal (SMART-T) for a highly survivable alternate means of reachback for Defense Information Systems Network services. SMART-T planning is a collaborative effort involving the network engineer, the spectrum manager, the key management infrastructure operations account manager, the regional satellite communications support center, and the Defense Information Systems Agency. (See TC 6-02.21)

### **Network Engineer**

3-21. The network engineer integrates the SMART-T into the unit's portion of the DODIN-A. The network engineer defines the requirements for the satellite access request and gateway access request, and determines the optimal location to employ the SMART-T, based on threat environment, service and survivability requirements.

3-22. The network engineer, in collaboration with the G3 or S3, provides the spectrum manager with information regarding mission; deployment timeline; supporting headquarters requirements and services; outside the continental United States or continental United States mission; host-nation agreements and landing rights approval information; area of operations; and terrain in the area of operations.

### **Spectrum Manager**

3-23. The spectrum manager uses the requirements provided by the network engineer to generate a satellite access request and a gateway access request. The spectrum manager submits the satellite access request to the regional satellite communications support center serving the deployed area of operations, and the gateway access request to the Defense Information Systems Agency Contingency and Exercise Branch, using the Joint Integrated Satellite Communications Tool over SIPRNET. When the unit receives an approved satellite access authorization, the spectrum manager adds the frequencies to the spectrum database for deconfliction with other known emitters.

### **Regional Satellite Communications Support Center**

3-24. The regional satellite communications support centers provide planning, engineering, and satellite payload management for all military satellite communications systems. The regional satellite communications support centers' staffing includes personnel from the Army, Navy, Air Force, and the Defense Information Systems Agency.

3-25. The regional satellite communications support center servicing a deployed area of operations validates and approves or disapproves satellite access requests in its service area based on mission priority and availability of satellite resources. If the regional satellite communications support center approves the requests, it generates a satellite access authorization and distributes it to the requesting unit and the terminal segment, control segment, and DOD gateway elements supporting the mission.

### **Defense Information Systems Agency**

3-26. The Defense Information Systems Agency Contingency and Exercise Branch provides guidance, manages strategic resources, and coordinates usage of Defense Information Systems Network services. The Contingency and Exercise Branch processes gateway access requests and issues gateway access authorizations to extend pre-positioned Defense Information Systems Network services through DOD gateway sites to support global requirements. The Defense Information Systems Agency manages teleports to support satellite network management.

### **Key Management Infrastructure**

3-27. (U) Key management infrastructure is the framework and services that provide the generation, production, storage, protection, distribution, control, tracking, and destruction for all cryptographic keying material, symmetric keys as well as public keys and public key certificates (CNSSI 4005). Key management infrastructure provides a unified, interoperable, and trusted infrastructure for establishing, using, operating, and managing cryptographic products and services in a net-centric environment (ATP 6-02.75).

3-28. A key management system generates, distributes, and manages cryptographic keys for devices and applications. This system may cover all aspects of security from the secure generation of keys, secure exchange of keys, to secure key handling and storage on the client workstation. A key management system includes functions for key generation, distribution, and replacement, as well as client functionalities for injecting, storing, and managing keys on devices. Refer to ATP 6-02.75 for planning and implementation of cryptographic networks.

## **NARROWBAND (SINGLE-CHANNEL) SATELLITE COMMUNICATIONS**

3-29. Narrowband (single-channel) satellite communications support long-range tactical network transport for en-route contingency communications, in-theater communications, fire support networks, and combat net radio range extension. Planners should submit a satellite access request 30–45 days before the mission to allow adequate time for processing. Planners use the Joint Integrated Satellite Communications Tool on SIPRNET to prepare and submit satellite access requests for narrowband satellite communications service. Refer to ATP 6-02.53 for more information about single-channel satellite communications radios.

## **LINE-OF-SIGHT TRANSPORT**

3-30. Line-of-sight transport can handle much higher data rates than satellite communications systems, but are range limited by the curvature of the Earth, terrain, and other natural or man-made obstructions. Line-of-sight radio planning requires careful terrain analysis between proposed signal sites during site selection to ensure the transmission path is unobstructed and to minimize the chances of an enemy intercepting or jamming the signal.

## **HIGH THROUGHPUT LINE-OF-SIGHT TRANSPORT**

3-31. High-throughput line-of-sight radios can carry high bandwidth data over distances up to 25 miles, but the links need to be engineered to minimize the chance of detection, targeting, and jamming. If the line-of-sight path is parallel to the forward line of troops, an enemy is less likely to detect the signal, and enemy jammers will be unable to reach the antenna with a signal strong enough to jam the radio (FM 6-02).

## **TERRESTRIAL TRANSMISSION LINE OF SIGHT**

3-32. Terrestrial Transmission Line of Sight provides high-bandwidth, low latency transportable communications using reduced size, weight, and power. Terrestrial Transmission Line of Sight extends the existing WIN-T network, reducing the reliance on satellite communications, and allows connectivity where satellite resources are not available. Terrestrial Transmission Line of Sight provides a small form factor, low latency, high-throughput terrestrial capability that increases network reliability.

## **HIGHBAND NETWORKING RADIO**

3-33. The Highband Networking Radio delivers high rate data throughput on-the-move and at-the-halt and enables automatic connection to other Highband Networking Radio-equipped nodes in WIN-T increment 2. Planning techniques for the Highband Network Radio are the same as for other line-of-sight radios.

3-34. The division and brigade headquarters are equipped with the Tactical Relay-Tower to extend the range of the Highband Networking Radio. The Tactical Relay-Tower operates as a standalone unit or in conjunction with a co-located tactical communications node. The Tactical Relay-Tower extends the range of the Highband Networking Radio to as much as 30 kilometers with an unobstructed line of sight. The Tactical Relay-Tower operates at the-halt only. The Tactical Relay-Tower sends and receives colorless enclave data over the highband networking waveform. The Tactical Relay-Tower provides no networking capabilities or user services for either SIPRNET or NIPRNET.

## **TROPOSPHERIC SCATTER**

3-35. Tropospheric scatter, or troposcatter, enables communications with microwave radio signals over distances of nearly 200 miles by randomly scattering ultrahigh frequency and super high frequency radio waves as they pass through the upper atmospheric layers of the troposphere. Troposcatter transmits radio signals in a narrow beam aimed just above the horizon in the direction of the receiver station. As the signals pass through the troposphere, some of the energy scatters back toward the receiver station.

## COMBAT NET RADIOS

3-36. Combat net radios include tactical radio systems that provide voice and data communications to support mobile, mounted, dismounted and command post communications. Combat net radio nets typically include platoon and squad radio systems such as Nett Warrior; handheld; vehicle and aircraft SINCGARS; and single-channel tactical satellite communications. Combat net radios provide the capability to extend voice and data services to individual users and platforms, and extend coverage to the digital network. Combat net radios are comprised of intra-squad radios, SINCGARS, and single-channel tactical satellite communications radios. Combat net radios provide the capability to extend frequency modulation network coverage to the digital network.

## SINGLE-CHANNEL GROUND AND AIRBORNE RADIO SYSTEM

3-37. The SINCGARS provides the primary means of communication for units across all echelons using highly reliable, secure, easily maintained combat net radio voice and data handling capability. The SINCGARS offers network data services using mounted, dismounted, and airborne configurations.

## SINGLE-CHANNEL TACTICAL SATELLITE

3-38. Single-channel tactical satellite provides interoperability between legacy tactical satellite radios and software defined radios. Single-channel tactical satellite provides the capability for users to interoperate with legacy radio waveforms. The interoperability enables voice and limited data exchange for beyond line-of-sight at the lowest tactical level users in the lower tier.

## HANDHELD, MANPACK, AND SMALL FORM FIT

3-39. The handheld, manpack, and small form fit radio program provides joint single-channel handheld and two-channel manpack radios and consist of handheld radios and manpack radios. The handheld radios consist of legacy single-channel radios operating Soldier radio waveform, and the two-channel Leader Radio, using both legacy SINCGARS and Tactical Scalable Mobile Ad Hoc Networking waveforms. The manpack radios consist of the generation 1 Soldier radio waveform, legacy satellite communications, SINCGARS, and Mobile User Objective System. For more information on the handheld, manpack, and small form fit radio program, refer to ATP 6-02.53.

## RADIO RETRANSMISSION

3-40. Retransmission extends radio communications around obstructions and beyond line-of-sight range. Retransmission assets support command and control, administrative and logistics, operations and intelligence, and fires networks.

3-41. Retransmission operates on the command network to subordinates unless specifically tasked to operate on another network. The primary radio monitors the command and operations, and intelligence networks. The secondary radio provides the retransmission link.

3-42. SINCGARS operates as either a single-channel secure or a single-channel nonsecure retransmission station. The retransmission radio automatically passes single-channel secure signals even if the retransmission radios are operating in nonsecure mode. The retransmission operator cannot monitor the communications unless the secure devices are filled and in the cipher mode.

3-43. Considerations for retransmission planning include—

- Contingency planning.
- Quick reaction force and relocation evacuation criteria.
- Casualty evacuation plan.
- Alternate locations.
- Compromise procedures.
- Reseed plan (vehicle, radios, and personnel).

3-44. Planners should also consider advanced coordination for establishing security plans, sleep plans, logistics coordination for fuel, meals, maintenance repair, reporting requirements, and no fire areas.

3-45. Retransmission teams are vulnerable to enemy attack due to failure to control emissions using electromagnetic masking and failure to use cover and concealment or camouflage. Radios placed on low power offer the best emission control. Refer to ATP 6-02.53 and the Radio Operators Handbook for detailed information about retransmission. Another resource for retransmission planning is the Graphic Training Aid 11-02-001, *Retransmission Mission Checklist*.

3-46. Retransmission normally requires the following equipment:

- Two Advanced System Improvement Program radios.
- AN/VRC-92 configuration.
- CX-13298 retransmission cable.
- Two OE-254 or COM-201B antennas.

3-47. Planners may configure retransmission networks as either the same network identification or different network identification. Using different network identification provides a relay to extend communication range and allows both radios to transmit and receive.

3-48. While planning radio retransmission, planners may consider using the same network identification. This enables radio A to receive and transmit while radio B can either receive or transmit. Radio A and B frequency must have 10 megahertz or greater frequency separation. See figure 3-2.

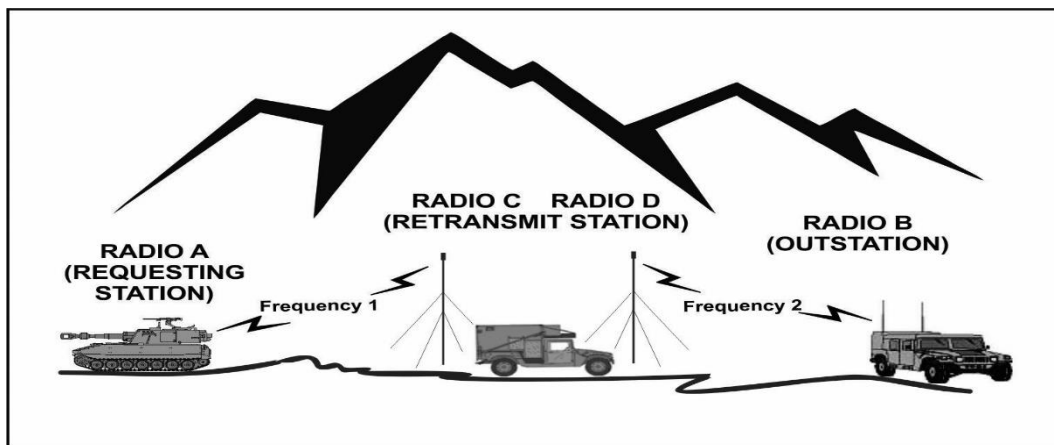


Figure 3-2. Retransmission operations

## HIGH FREQUENCY RADIOS

3-49. High frequency (HF) radios provide tactical elements with stand-alone, terrain independent, robust communications for line of sight and beyond line-of-sight secure voice and data communications. *Line of sight* is the unobstructed path from a Soldier's weapon, weapon sight, electronic sending and receiving antennas, or piece of reconnaissance equipment from one point to another (ATP 2-01.3).

3-50. HF radios provide long distance, wide area, gap-free, fixed or on-the-move, ground-to-ground, and ground-to-air communication. HF radios are terrestrial beyond line-of-sight systems that require a good understanding of HF capabilities and antenna design to communicate either line of sight or beyond line-of-sight. HF radios provide a combination of simplicity, economy, transportability, and versatility.

3-51. HF radios have the following characteristics that make them ideal for tactical long distance communications:

- HF signals reflected off the ionosphere at high angles allow beyond line-of-sight communications at distances up to 400 miles (643.7 kilometers) without gaps in communications coverage.
- HF signals reflected off the ionosphere at low angles allow communications over distances of many thousands of miles.



- HF signals do not require using either satellite communications or retransmission assets.
- HF systems operate independently of intervening terrain or man-made obstructions.

3-52. Training Soldiers on the operation and use of HF radios plays a vital role in successfully accomplishing units' missions. Communications planners at every level need to understand radio wave propagation, path loss, antennas, antenna couplers, and digital signal processing. Refer to ATP 6-02.53 for detailed information about single-channel radio operation.

## LINK-16

3-53. Link-16 is an encrypted, jam-resistant tactical data link network used by U.S. and North Atlantic Treaty Organization allies to create situational awareness among dispersed battle elements by sharing information over a common communications link. This enables command and control centers to create a common operational picture, which allows friendly forces to visualize the battlespace, identify threats, and acquire targets.

3-54. Link-16 communications transfer real-time combat data, voice communications, imagery, and relative navigation information on the battlefield. This network uses joint tactical information distribution system-compatible communications terminals to transmit and receive data messages. Link-16 network messages broadcast simultaneously to as many users as needed. Link-16 is a nodeless network that does not depend on any single terminal to act as a node. Link-16-capable terminals act as nodes.

3-55. The primary application of Link-16 is air and missile defense command and control systems. Various countries use the Link-16 network for national air defense, to link their sea- and land-based vessels, ground-based sensors, and surface-to-air missile systems.

## INFORMATION SERVICES

3-56. Information services allow authorized access, storage, and sharing of information among mission partners, as well as dynamically tailoring and prioritizing information to support the mission and affect the operational environment (FM 6-02). Tactical signal systems deliver classified and non-classified voice, video, and data services—including Defense Information Systems Network Services—needed to enable situational understanding, staff planning, and coordination. Information services consist of—

- **Messaging services** enable the exchange of information among users. Messaging services include e-mail, Organizational Messaging Service, instant messaging, and alerts.
- **Discovery services** enable discovery of information content or services stored in directories, registries, and catalogs. An example of a discovery service is a search engine.
- **Mediation services** enable system interoperability by processing data to translate, aggregate, fuse, or integrate it with other data.
- **Collaboration services** provide the ability for warfighters to work together and share capabilities. Examples of collaboration services are chat, online meetings, and workgroup applications.
- **Storage services** provide physical and virtual data hosting. Storage services include archiving, continuity of operations, and content staging. Standard operating procedures or operation orders should define information storage locations.
- **User assistance services** provide centralized service desk assistance and automated access to lessons and best practices, which may improve processes or reduce the effort required to perform tasks.
- **Identity and access management** (Enterprise Directory Service) provides authoritative enterprise identity and contact attributes for combatant commands, Services, and agencies. Enterprise Directory Service includes—
  - DOD Enterprise White Pages—authoritative identity and contact information for all DOD common access card holders.
  - Global Directory Service—a distribution point for personal public key certificates, certificate revocation lists, and certificate authority certificates.

- Identity Synchronization Service—populates directories and global address lists with enterprise identity and contact attributes.
- **User assistance services** provide centralized service desk assistance and automated access to lessons and best practices, which may improve processes or reduce the effort required to perform tasks.
- **Identity and access management** (Enterprise Directory Service) provides authoritative enterprise identity and contact attributes for combatant commands, Services, and agencies. Enterprise Directory Service includes—
  - DOD Enterprise White Pages—authoritative identity and contact information for all DOD common access card holders.
  - Global Directory Service—a distribution point for personal public key certificates, certificate revocation lists, and certificate authority certificates.
  - Identity Synchronization Service—populates directories and global address lists with enterprise identity and contact attributes.

3-57. Information services also support joint, inter-organizational, and multinational collaboration. Information sharing allows the mutual use of information services or capabilities across functional or organizational boundaries.

3-58. Identity and access management services facilitate and control information sharing. Identity and access management assigns users common, portable identity credentials, such as a common access card or SECRET Internet Protocol Router Network token. Users with the proper credentials can access and view operational, business support, or intelligence-related information, services, and applications related to their mission and communities of interest. Refer to ATP 6-02.71 for more information about information services.

## **REGIONAL HUB NODE OR DEPARTMENT OF DEFENSE GATEWAY COORDINATION**

3-59. Planners should conduct several coordination calls leading up to each exercise or mission that uses the regional hub node or DOD gateway for access to the DODIN-A and Defense Information Systems Network services. Coordination ensures the regional hub node or gateway site can adequately support the mission.

3-60. Preparation for significant training events should include regional hub node leadership for proper command emphasis. This leads to increased technical and field service representative support at the regional hub nodes during the training event.

3-61. The United States Army Communications-Electronics Command provides regional hub node playbooks with detailed configuration information that serve as technical guides for installation and troubleshooting. The regional hub node playbooks are available at the ACAS Website.

## **SECTION II – NETWORKING**

3-62. Networking encompasses several components to ensure availability. Army network planners should consider cybersecurity, internet protocol planning, allocation, and quality of service. Early planning is key to successful network planning.

## **CYBERSECURITY**

3-63. *Cybersecurity* is prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation (DODI 8500.01).

3-64. Cybersecurity sets the baseline security posture of the network to protect against known exploits and vulnerabilities, rather than a particular threat actor or capability. Cybersecurity ensures information technology assets provide mission owners and operators confidence in the confidentiality, integrity, and availability of information systems and information, and their ability to make choices based on that

confidence. The DOD cybersecurity framework provides the foundation for the cybersecurity program. Refer to ATP 6-02.71 for detailed information about the cybersecurity framework.

## SECURITY DOMAIN

3-65. A security domain is a system or network, such as NIPRNET, SIPRNET, or Joint Worldwide Intelligence Communications System, that operates at a particular sensitivity level. Transferring data between security domains, for example between NIPRNET and SIPRNET, requires a cross domain solution. A *cross domain solution* is a form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains (CNSSI 4009). Cross domain solutions need careful control because of the damage that can result due to spillage from a higher domain to a lower classification, for example secret information spilled onto NIPRNET.

## INTERNET PROTOCOL PLANNING

3-66. Effective Internet protocol (IP) address allocation requires diligent planning and relatively accurate forecasting. Knowing the IP address space requirements for the network enables network planners and engineers to allocate address space to meet the commander's requirements while minimizing wasted addresses. Accurate long-term IP address forecasting is seldom possible. Mission requirements drive continual change with the opening of new sites, closing or moving sites, and implementing new initiatives, such as voice over internet protocol telephony.

3-67. Beyond strategic events that can usually be preplanned, organizational dynamics can drive short-term stress in address capacity requirements. Network engineers should map out high-level address capacity requirements, allowing some reserve address space if possible. DODIN operations elements monitor address utilization to ensure effective use of the addresses allocated, given the short- and long-term address-affecting events. Monitoring may indicate the need to reallocate addresses to meet urgent or emergent requirements.

3-68. The intensity of monitoring should relate directly to the rate of address space utilization. Networks above 90 percent utilization may need monitoring hourly or at least multiple times per day. Networks with utilization below 70 percent need less frequent monitoring.

3-69. Network engineers define alert thresholds within a monitoring or IP address management system to alleviate the need for continuous monitoring. Beyond capacity requirements, another important consideration is the hierarchical allocation of IP address blocks so address space rolls up to the highest level efficiently.

## ALLOCATION BY APPLICATION

3-70. Certain applications and data types, such as voice and video, require low latency to operate correctly. On the other hand, data transmission can tolerate multi-second delays. Network planners should implement routing based on the application and type of data. One way to perform this is to allot a portion of the overall address space to treat voice with higher priority queuing, while separating this from the data space. Other protocol-specific applications may need further address delineation.

## DYNAMIC HOST CONFIGURATION PROTOCOL

3-71. Dynamic Host Configuration Protocol (DHCP) is a client-server protocol to automatically allocate an IP address for devices connecting to a network. DHCP can simplify and speed command post initialization, since automation personnel does not need to manually configure and add each user to the switch. However, using DHCP during normal operation creates an opportunity for unknown users to connect to the network. For this reason, network managers should disable DHCP and implement port security as soon as the digital command post footprint and primary users are established (ATP 6-02.60).

3-72. DHCP enables a device to broadcast its request for an IP address, and have one or more DHCP servers in the network service the request without user or network administrator intervention. For most end-user devices such as laptops and Voice over Internet Protocol phones, the DHCP process takes place automatically behind the scenes upon device boot-up or connection to a wired or wireless network connection.

3-73. DHCP also enables efficient use of IP addresses by allowing an IP address to be reused among devices within dynamically allocated address pools. An IP address may be used by one device one day and a different device the next. DHCP supports three types of IP address allocation—

- Automatic allocation—the DHCP server assigns a permanent IP address to the client.
- Manual allocation—the DHCP server assigns a fixed IP address, based on the device's hardware address.
- Dynamic allocation—the DHCP server assigns an IP address for a limited time, after which the address can be reassigned.

3-74. Automatic allocation may be useful for a particular set of users or devices requiring a permanent IP address assignment using DHCP, where there is no requirement for devices to have a specific IP address. Planners should consider reserving a set of permanent addresses with no associated DHCP address.

3-75. Manual allocation requires the administrator to associate a particular hardware address with a corresponding IP address. Typically, the administrator bases manual DHCP on a predefined mapping scheme.

3-76. Dynamic allocation configures address pools in DHCP servers to reuse IP addresses. The DHCP server leases its IP addresses to clients for a fixed period and assigns an IP address to a particular client for a given time period.

## **FIREWALLS**

3-77. A firewall is a network security device that monitors incoming and outgoing network traffic and grants access to the network based on approved local policies. Network firewalls provide network security against threats and ensure a resilient network.

3-78. G-6 and S-6 personnel assigned to the DODIN operations section normally configure firewalls based on defined guidelines. Firewalls protect networks from unauthorized intrusions that may harm the network. Considerations for planning firewalls include the following—

- Identify security requirements for your organization.
- Define an overall security policy.
- Define a firewall philosophy.
- Identify permitted communications.
- Identify the firewall enforcement points.

## **QUALITY OF SERVICE**

3-79. When available network bandwidth is relatively fixed, it is important to allocate it effectively. WIN-T handles several different types of data with varying importance and transmission requirements. For example, in an IP network, voice and video become digital packets during transmission similar to e-mail. Delays in voice or video packets during transport are not acceptable. Video can become choppy and not viewable, and voice calls can become garbled. On the other hand, packets comprising an e-mail eventually arrive intact with no recognizable consequence of time delays.

3-80. Some sources of data are more time-critical than other sources. Quality of service is a networking approach that helps optimize available bandwidth. It gauges user demand to maintain effective throughput. Quality of service edge devices provides the means to manage bandwidth-constrained traffic, taking into account both time criticality and information importance. Quality of service mechanisms help manage resources to avoid network bottlenecks, and ensure that both quality and speed of service meet user requirements.

## **INFORMATION DISSEMINATION MANAGEMENT AND CONTENT STAGING**

3-81. Information dissemination management and content staging emplace, manage, provide, and restore information services to enable information and knowledge management. Information dissemination management supports effective knowledge management so the right information reaches the right users at

the right time, in a usable format. Content staging compiles, catalogs, and caches information. The Army task of information dissemination management and content staging corresponds to, and nests within, the joint task of DODIN content management. Information dissemination management and content staging (DODIN content management) allow users to retrieve, cache, compile, catalog, and distribute information to support planning and decision making. Information dissemination management and content staging consist of the technologies, techniques, processes, policies, and procedures to provide—

- Awareness of relevant, accurate information.
- Automated access to newly revealed or recurring information.
- Timely, efficient, delivery of information in a usable format.
- The DODIN operations essential tasks take place at the strategic, operational, and tactical levels and support all warfighting and business functions. DODIN operations enable network and system availability, information protection, and timely information delivery across strategic, operational, and tactical boundaries.

## **NETWORK HARDENING**

3-82. Network hardening ensures the confidentiality, integrity, and availability of network services. A hardened network mitigates enemy entry into the DODIN-A. Commanders and staffs ensure their network is secure and accessible to all approved and validated users.

3-83. Network planners should consider implementation of a zero trust architecture. Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero trust architecture is an enterprise's cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies. National Institute of Standards and Technology Special Publication 800-207 provides detailed implementation guidance for zero trust architecture.

### **Strong Authentication**

3-84. Reducing anonymity as well as enforcing authenticity and accountability for actions on the DODIN-A improves the security posture of the network. The connection between weak authentication and account seizure is well known and established. Strong authentication helps prevent unauthorized access, including wide-scale network compromise by impersonating privileged administrators. Commanders and supervisors focus on protecting high-value assets, such as servers and routers, and privileged system administrator access.

### **Device Hardening**

3-85. Proper hardening of network devices increases the cost and complexity of adversary exploitation. Network managers prevent common exploitation techniques through proper configuration, vulnerability patching, and disabling active content in e-mails. Planners should ensure updated device patching prior to entering an area of operations. A defense in depth approach places layers of defensive measures to slow down or stop the adversary from entering the network. These measures are critical to thwarting an adversary's attempts to escalate privileges and maneuver freely within DOD networks.

3-86. Device vulnerabilities are exploitable weaknesses in software or hardware that provide an adversary an opportunity to compromise the confidentiality, integrity, and availability of an information system. Adversaries attempt to exploit vulnerabilities for various purposes, including accessing, modifying, deleting or exfiltrating sensitive information, modifying system configurations, installing malicious code, or denying system access to authorized users.

### **Reduced Attack Surface**

3-87. The attack surface of the DODIN-A has many aspects that must be addressed to improve cybersecurity readiness. Commanders and supervisors mitigate the vulnerabilities associated with Internet-based adversaries by eliminating Internet-facing servers from the DODIN core, ensuring Internet-facing servers in DOD demilitarized zones are operationally required, and removing trust relationships with external

authentication services. If adversaries gain access to systems within a DOD demilitarized zone, they must be prevented from exploiting active directory trust relationships to gain elevated privileges inside the DODIN. This requires the proper management of trust relationships between DOD enclaves. Commanders and supervisors must ensure only authorized devices can access DOD infrastructure, either physically or logically.

3-88. Hardening the DODIN-A from threats increases network reliability. Network planners configure devices and peripheral equipment to ensure the network is secure and available for users. Planners enable and configure network traffic monitoring and endpoint security to detect and prevent threats to the DODIN-A. Table 3-1 on page 3-15 contains suggested network hardening techniques.

Table 3-1. Network hardening techniques

Domain Management and Security	Network Device Management and Security	Network Traffic Monitoring and Alerts	Endpoint Security
Create and Design Organizational Units	Configure Solar Winds Network Configuration Manager (WNM Server)	Configure Solar Winds NetFlow Traffic Analyzer	Deploy Host Base Security System
Grant Access Based on Role-Based Authentication	Configure Universal Threat Manager (Cisco Security Manager)	Configure Devices to Send Logs/Alerts to ESM	Configure Host Base Security System Dashboards
Enable File Server Resource Manager	Load Current Device Configurations/Policies Using Cisco Security Manager	Build Connectors in ESM for Logs/Alerts from Devices	Assured Compliance Assessment Solution Deployment and Scanning
Configure Distributed File System (Create Share Drives)	Configure Layer 2 Security Features	Enable ESM Log Forwarding to RCC/Higher Level Command	Establish Patch Management Policies and Procedures
Establish and Configure Print Servers	Verify Additional Layer 2 Security Checks (Remove Type 7 passwords)	ESM Alerts and Dashboard Configurations	Windows Deployment Service Configuration
Create Group Policy Objects		Configure Security Onion	Establish Password Security on Printers
Setup Folder Redirection for VIPs			Change ALL Default Passwords on Endpoints
Deploy a Read-Only Domain Controller			Deploy Host Base Security System
Implement a Test Environment for GPOs and Security Changes			
Implement a Local Change Control Board			
<b>Legend:</b> ESM            Endpoint Security Manager GPOS        group policy objects RCC        regional cyber center			

## SECTION III – SPECTRUM PLANNING

3-89. *Spectrum management operations* are the interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations (FM 6-02).

3-90. Spectrum management operations aim to ensure access to the electromagnetic spectrum in support of the Army's operational missions. Spectrum management operations enable cyberspace electromagnetic activities. Spectrum management is the operational, engineering, and administrative procedures to plan, coordinate, and manage use of the electromagnetic spectrum and enables cyberspace, signal and EW operations.

3-91. Spectrum management operations enable the management of allotted and limited frequencies directly supporting operational forces throughout the world. The Army is dependent upon the use of the electromagnetic spectrum at all echelons. Effective spectrum management operations enable electromagnetic systems to perform their functions in the intended environment without causing electromagnetic interference.

3-92. Spectrum planning includes the identification of spectrum requirements for training, pre-deployment, deployment, and reconstitution of Army forces, both within and outside the continental United States. Spectrum planning is a continual process that must be deliberate as well as dynamic. It requires the collection, storage, and protection of critical spectrum data, and assured access to this data by spectrum planners on a global scale. Additionally, planning for the establishment of communications and coordinating for spectrum use with national and international governmental and non-governmental entities is critical to spectrum planning.

3-93. Spectrum managers use various tools to manage and plan the unit's spectrum needs and objectives. Examples include—

- Automated Communications Engineering Software and Joint Automated Communications System.
- Afloat Electromagnetic Spectrum Operations Program.
- Electronic Warfare Planning Management Tool.
- Host-Nation Spectrum Worldwide Database Online.
- Joint Automated Communications-Electronics Operation Instructions System.
- Spectrum Situational Awareness System.
- Systems Planning, Engineering, and Evaluation Device.
- Coalition Joint Spectrum Management Planning Tool.

## **FREQUENCY DECONFLICTION**

3-94. *Frequency deconfliction* is a systematic management procedure to coordinate the use of the electromagnetic spectrum for operations, communications, and intelligence functions (JP 3-85). Frequency deconfliction is one element of electromagnetic spectrum management and applies practices to minimize or prevent spectrum-dependent devices from suffering or causing interference while being used as intended (ATP 6-02.70). Frequency deconfliction shares a common goal with electromagnetic interference mitigation. Spectrum managers conduct frequency deconfliction during the planning phase of a mission to prevent interference. Electromagnetic interference mitigation takes place when interference occurs during mission execution.

3-95. The G-6 or S-6 spectrum manager develops and maintains a database of all known emitters and receivers in the area of operations. This database identifies and prioritizes competing systems for frequency assignments. Spectrum managers review the database to deconflict frequencies and prevent interference.

3-96. Deconfliction ensures EW capabilities do not create unintended electromagnetic interference (frequency fratricide) with friendly communications, unmanned aircraft systems, weapon systems, or positioning, navigation, and timing. Failing to share situational understanding could cause planners or operations personnel to miss cyberspace or electromagnetic attack indicators. Spectrum managers use various tools to deconflict frequencies. Refer to ATP 6-02.70 for a list of tools available to spectrum managers for frequency deconfliction.

## **FREQUENCY ASSIGNMENT**

3-97. The spectrum manager receives spectrum resources in the form of allocation tables and permissions from higher echelons, such as the Army Spectrum Management Office, Joint Frequency Management Office,



or host-nation spectrum authorities. The spectrum manager uses management tools to transfer the information into the standard frequency action format or standard spectrum resource format and enters it into spectrum use databases.

## SIGNAL OPERATING INSTRUCTIONS

3-98. The single-channel radio planner uses Automated Communications Engineering Software (ACES) to plan radio networks and produce the signal operating instructions. Collection of data to support generation of first-time signal operating instructions for a division-sized element may take from 5 days to over 30 days. Building an initial master netlist to support first-time signal operating instructions generation takes 4–7 days. ACES normally generate the signal-operating instructions for a division in 2–5 hours.

3-99. The hopset provides frequency resources used in a loadset. The transmission security key determines the frequency hop pattern for the radio. Although the ACES automates the generation process, the signal officer, communications chief, and frequency manager design the signal operating instructions on paper first. Table 3-2 lists the initial data requirements to develop signal operating instructions.

**Table 3-2. Automated Communications Engineering Software signal operating instructions data requirements**

<b>Step</b>	<b>Description</b>
1	Research and extract data from the modified table of organization and equipment, which authorizes the use of personnel and equipment.
2	Determine the doctrine to be followed.
3	Develop operation order, operation plan, or unit standard operating procedure.
4	Frequency list from the spectrum manager.
5	Determine how many networks and frequencies the operation plan or order requires. Use existing signal operating instructions as a starting point.

## RADIO LOADSETS

3-100. G-6 or S-6 planners identify requirements for the construction of loadsets to support their organization's radio networks. The frequency manager constructs loadsets using ACES, saves them to file, and distributes them to subordinate units or elements for follow-on distribution to radio users. Loadsets provide radio network access and monitoring based on the user. A loadset consists of communications security (COMSEC) key tags, frequency hopsets, lockouts, and target definition, transmission security key and net identifiers.

3-101. For example, the commander of an infantry battalion is normally a member of several single-channel radio networks. One of the commander's radios could be preset to operate in all of the following networks:

- Brigade command network.
- Brigade operations network.
- Battalion command network.
- Battalion operations network.
- Brigade retransmission network.

## LOADSET UPDATES

3-102. Signal planners use ACES to manage loadset data. The loadset data is saved to a file, and distributed using a fill device to ensure they are in-place and available for loading into the SINCGARS at the appropriate key changeover time. Signal sections should have several loadsets with associated key constructed and distributed (or available for distribution) for immediate use.

3-103. Existing loadsets may require revision when the required network content changes (unit reassignment or attachment). New loadsets may require construction to meet new requirements (for example, create a new task force organization).

## JOINT-TACTICAL NETWORK OPERATIONS TOOLKIT

3-104. The Joint Tactical Network Operations Toolkit is the primary tool used to load mission plans onto tactical radios. The Joint Tactical Network Operations Toolkit laptop contains the Joint Enterprise Network Manager software used to create the mission plans on the laptop. The Joint Enterprise Network Manager provides the ability to load multiple radio mission plans rather than load each radio individually.

## HOST-NATION COORDINATION

3-105. Host-nation coordination is negotiation for authorization to operate radio frequency-emitting equipment within a sovereign nation. This coordination is necessary to conform to international and national laws, and to avoid interfering with host-nation communications and emergency services. Coordination prevents diplomatic friction with the host-nation (FM 6-02).

3-106. Host-nation coordination ensures initial spectrum availability and supportability for operations. Channels for coordinating spectrum allocation at the national and international levels adhere to policies established in the planning process. Spectrum managers coordinate with host-nation and adjacent countries' spectrum authorities, particularly if forces stage, train, or operate in adjacent countries. Coordination covers airspace, sovereign waters, and satellite communications frequencies. Coordination includes advance planning and continual collaboration during operations. Host-nation coordination does not apply to forcible entry operations or operations in a hostile nation. Refer to ATP 6-02.70 for detailed information about spectrum management operations.

## SECTION IV – COMMUNICATIONS SECURITY

### PLANNING CRYPTOGRAPHIC NETWORKS

3-107. *Communications security* are the 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 (JP 6-0).

3-108. G-6 or S-6 network managers may have the responsibility for planning the networks that consist of transmission systems, circuit switches, data switches, routers, and other devices. The signal unit has responsibility for engineering the networks. The network managers consider the objective of the mission, the units that will participate in the mission, type of communications required, and duration of the mission.

3-109. Establishment of a cryptographic network involves identifying operational requirements for a command or unit. For cryptographic devices to intercommunicate securely, all members of the network must use compatible equipment and associated keying material.

3-110. The network manager develops a communications plan to support the unit's operation order. The ACES operator uses the operation order or communications plan as a basis to plan cryptographic networks.

3-111. The ACES operator develops a cryptographic network overlay and identifies COMSEC requirements for the mission based on the operation order or communications plan. The COMSEC planner can tailor the ACES and workstation to meet a variety of planning requirements. The three network categories are combat net radio, Area Common User System, and general-purpose. There is a planning module for each network category.

3-112. The general-purpose planning module application develops a cryptographic network overlay for the mission based on the communications network. The COMSEC planner identifies and processes key material requirements through the general-purpose module application. General-purpose cryptographic networks exist independently of other networks. This provides the capability that manually creates special purpose cryptographic networks to meet any distinct need. The ACES operator delivers key requirements to the key management infrastructure operating account manager.

3-113. The local management device and key processor operator process key requirements; provide the necessary short title information concerning each key to add to the ACES cryptographic network overlay;

and pass this information to the ACES operator. When the plan is complete with the short titles, the key management infrastructure operating account manager returns the cryptographic plan to the ACES operator.

3-114. The ACES operator finishes processing the cryptographic network, and provides the cryptographic network plan along with the signal operating instructions and loadset data to end users. The key management infrastructure operating account manager generates and distributes red key to the end user by loading keys into the user's fill device. End users key the end cryptographic units from the fill device.

This page intentionally left blank.

## Chapter 4

# Signal Site Planning

This chapter discusses signal site planning. Section I discusses signal site analysis and site selection. Section II discusses site setup, including site reconnaissance, priorities of work, site security and defense, and command post signature reduction.

### SECTION I – SITE SELECTION

4-1. The operating characteristics, capabilities, and limitations of various communications systems dictate requirements for acceptable operating locations. Signal sites must be able to accomplish their assigned missions while remaining supportable and defensible.

### SIGNAL SITE ANALYSIS

4-2. A comprehensive site analysis enables the meaningful course of action comparison during planning and provides flexibility when executing operations. Signal site analysis and selection require collaboration between the G-6 or S-6, G-3 or S-3, and the G-2 or S-2:

- The G-6 or S-6 analysis focuses on the ability of communications systems to provide coverage from the proposed site.
- The G-3 or S-3 analysis focuses on mobility, survivability, and sustainability.
- The G-2 or S-2 analysis focuses on terrain and the threat situation.

4-3. Signal planners consider the operating characteristics, limitations, and effective planning distance for each available communications asset. Signal planners evaluate the terrain (including man-made features) in the operational area to visualize how they can support the mission. Planners can take advantage of terrain and structures for terrain masking to protect systems from enemy detection, but the same features can make some communications systems, such as line of sight radios, ineffective. Planners consider the current threat estimate to prevent placing communications sites near known or anticipated enemy positions.

4-4. As planners define communications requirements, the number of retransmission sites needed to cover the area of operations may help determine the supportability of proposed courses of action during the military decision-making process.

### LINK GEOMETRY

4-5. The G-6 or S-6 analyzes the terrain to determine how to make the geometry of the operations work in favor of friendly forces. Improper link geometry makes it easier for the enemy to use direction finding and jamming capabilities.

4-6. When possible, terrestrial line of sight communications links should parallel the forward line of own troops. This keeps the primary signal strength of U.S. transmissions in friendly terrain. Deploying units and communications systems with the transmission path perpendicular to the forward line of own troops aims transmissions toward the enemy and makes it easier for the enemy to jam or intercept communications.

### TERRAIN MASKING

4-7. When possible, command post locations should place terrain features and manmade structures between friendly communications systems and enemy positions. This may require moving senior headquarters farther forward and using more tactical command posts to ensure commanders can continue to direct their units effectively.

## **ANTENNA PLACEMENT**

4-8. Command post locations generally determine antenna locations. The proper installation and positioning of antennas around command posts are critical. G-6 or S-6 planners and system operators should position antennas and radio frequency emitters as far as practical from the command post to spread out the electromagnetic signature.

## **SITE SELECTION**

4-9. Selecting the right location for a command post is critical to its survivability. Poor placement can result in limited flexibility, limited mobility, enemy detection, degraded survivability, and reduced effectiveness. Site selection considers the mission variables METT-TC. Based on the signal site analysis, the G-6 or S-6 recommends a signal site for each proposed course of action during the military decision-making process. The final site selected must be—

- Able to support the selected course of action.
- Logistically supportable.
- Defensible—
  - Defensive plan.
  - Escape routes.
  - Cover.
  - Concealment.

4-10. Operating against a peer threat may require locating signal sites away from the supported command posts. This way, if an enemy locates and destroys communications systems, they do not destroy the entire command post capability. When placing signal systems away from the supported command post, planners must consider additional physical security and site defense requirements.

## **SECTION II – SITE PLANNING**

4-11. Planners should prepare a proposed site diagram showing the site layout of all signal assemblages, including the routing of all signal and power cables, and a plan for the use of a 30-meter antenna mast. Planning cable routes ensures sufficient separation between signal and power cables to prevent signal loss due to power hum on signal cables.

4-12. Signal site planning includes preparing a site layout. Planners may include marking locations with stakes to indicate parking locations for each signal assemblage. Planners identify and map proposed assemblage and antenna locations using 10-digit grid coordinates.

4-13. Planners identify the access road to the site and buried cable points. This allows adding new signal assemblages to the site without disrupting communications.

4-14. All designated ground guides and supervisory personnel should understand the site layout and the designated entry routes into the site. Ground guides direct the signal assemblages to their site positions by the designated routes and provide organized and speedy movement onto the site.

4-15. The G-6 or S-6 must know the effective planning distance for each available communications asset. Conducting an effective evaluation of the terrain and developing a visual understanding of how to support the mission is critical to the planning process.

4-16. The G-6 or S-6 coordinates with the G-2 or S-2 to determine the vulnerability of anticipated communications locations due to enemy capabilities. The G-2 or S-2 creates the enemy situation template used to ensure communications sites are not on or near known enemy positions.

## **SITE RECONNAISSANCE**

4-17. Before occupying a signal site, leaders should reconnoiter the designated area. The site reconnaissance might find unanticipated conditions that make the selected site unacceptable. This would require adjusting the operation plan or order to select a new signal site. The reconnaissance team should consist of the company

leader, the transmission supervisor (if applicable), node supervisor (if applicable), and a security team. The makeup of the reconnaissance team depends on the type of unit. The reconnaissance team maintains single-channel radio communications with their parent headquarters. The reconnaissance team should—

- Ensure the selected site can support the unit's communications requirements.
- Ensure the site is large enough to accommodate and tactically disperse all communications assemblages on the site.
- Determine whether the selected site is securable and defensible. The reconnaissance team considers—
  - The size of the site.
  - The number of personnel available to defend the site.
  - Entrances and avenues of approach.
  - Concealment from major roads or other vantage points. This may involve traveling around the entire site from a distance to visualize what the enemy would see.
- The reconnaissance team should verify the site is close enough to the supported unit command post to connect with the signal systems. Increasing distance between signal assemblages and subscribers complicates troubleshooting.
- The reconnaissance team should verify line of sight between stations for multichannel radio links. Line of sight planning range is about 25 miles (40 kilometers).
- The reconnaissance team should ensure terrain and man-made structures will not interfere with communications equipment and links.

4-18. If the situation does not allow for a leader's reconnaissance, leaders use the available information system resources such as line of sight analysis tools and satellite imagery to evaluate the proposed site. Considerations for selecting a command post location include—

- Establishing site security and defense.
- Communicating with higher, subordinate, and adjacent headquarters.
- Determining the range of enemy weapon systems.
- Gaining accessibility to passable entry and departure points (even in poor weather).
- Using terrain for passive security (cover and concealment) and terrain masking.
- Avoiding prominent terrain features (hilltops and crossroads).
- Co-locating with tactical units for mutual support and local security.
- Exercising command and control over subordinate and supporting units.

## PRIORITIES OF WORK

4-19. Standard operating procedures generally dictate unit priorities of work. However, the commander may change the priorities of work based on the mission variables METT-TC. If there are not enough Soldiers available to perform all of the tasks associated with setting up a command post and site security, established priorities help leaders determine the most important tasks to accomplish first. Clear priorities of work ensure personnel complete the key tasks to establish and secure the command post. Signal leaders continuously supervise the setup of communications systems to ensure crews follow the priorities of work.

### COMMAND POST SETUP

4-20. When erecting a command post it is important to follow the priorities of work. Priorities of work for command post setup, when trained and written into unit standard operating procedures, improve setup times, promote uniformity, and reduce missed steps (ATP 6-0.5).

4-21. Setting up a command post is a team effort. Responsibility for the command post set up typically goes to the operations sergeant major or the senior noncommissioned officer. During command post setup, all personnel should fall under the control of the senior noncommissioned officer to ensure quick and efficient setup operations. All personnel must be trained and have experience setting up the command post, both internally and externally. Refer to ATP 6-0.5 for more information about command post organization and establishment. Generally, command post set up priorities of work follow the order listed:

- Priority 1—Clear the site and establish security.
- Priority 2—Occupy the site.
- Priority 3—Establish tactical voice communications.
- Priority 4—Emplace the command post infrastructure.
- Priority 5—Emplace camouflage.
- Priority 6—Set up power generation grid and install power.
- Priority 7—Set up internal equipment (tables, chairs, lights, and map boards).
- Priority 8—Emplace and install networking and data equipment.
- Priority 9—Install mission command information systems.
- Priority 10—Establish sleeping and mess areas.
- Priority 11—Improve defensive positions.

4-22. Site set up and occupation requires advanced planning. Units establish local procedures for conducting site set up and publish procedures in unit standard operating procedures. Figure 4-1 on page 4-5 provides a sample diagram of signal site layout and site defense.

## **LINK ESTABLISHMENT**

4-23. The G-6 or S-6 determines and documents link establishment priorities for the network. These priorities ensure signal teams establish the most critical network capabilities to support the commander's intent and the main effort first. Priorities of work should always support the next higher echelon. That is, an individual team's priorities support the section or platoon. The platoon's priorities support the company. The G-6 or S-6 priorities must support the G-3 or S-3 and the commander's priorities. Figure 4-1 on page 4-5 shows a sample of link establishment priorities.



CODE				
LINK CODE				
SX	Satellite	SF=FDMA, ST=TDMA, SM=SMART-T FT=TFOCA, FS=Single Mode, FM+Multimode LH-HCLOS, Li=IPLOS CC=CatV, CX=CX11230		
FL	Fiber			
L	LOS			
CX	Cable			
		Nodes		
		Hub	00	
		JNN 7747	47	
		JNN 7748	48	
		CPN 77472	72	
		CPN 77473	73	
		CPN 77474	74	
		CPN 77475	75	
		CPN 77476	76	
		CPN 77477	77	
		Node 78	78	
		Node 79	79	
LINK ESTABLISHMENT PRIORITY				
Priority	Link	Adjacent Nodes	In Time	Remarks:
1	St47	00, 48, 72, 73, 74, 75, 76, 77		TDMA mesh established allowing all 2BCT nodes to connect to each other and hub.
1	ST48	00, 47, 72, 73, 74, 75, 76, 77		
1	ST72	00, 47, 48, 73, 74, 75, 76, 77		
1	ST73	00, 47, 48, 72, 74, 75, 76, 77		
1	ST74	00, 47, 48, 72, 73, 75, 76, 77		
1	ST75	00, 47, 48, 72, 73, 74, 76, 77		
1	ST76	00, 47, 48, 72, 73, 74, 75, 77		
1	ST77	00, 47, 48, 72, 73, 74, 75, 76		
2	SF4700			JNN FDMA connectivity to hub.
2	SF4800			JNN HCLOS backbone.
3	LH4748	48		CPN 7745 fiber link to 7747
3	LH4847	47		JNN SMART-T redundant links to each other
4	FT4775	75		
4	FT7547	47		
5	SS4748	48		
5	SS4847	47		
Legend				
BCT	brigade combat team			
CatV	category 5e cable			
CPN	command post node			
FDMA	frequency division multiple access			
HCLOS	high capacity line of sight			
IPLOS	internet protocol line of sight			
JNN	Joint Network Node			
LOS	line of sight			
SMART-T	Secure Mobile Anti-Jam Reliable tactical Terminal			
TDMA	time division multiple access			
TFOCA	tactical fiber optic cable assembly			

Figure 4-1. Sample link establishment priorities

## SITE SECURITY AND DEFENSE

4-24. Site defense planning depends on the size and type of signal site and whether it is co-located with the supported unit. Planners coordinate with the G-2 or S-2 staff for the current threat estimate and the G-3 or S-3 staff for security force requirements when planning site defense.

## CO-LOCATED SITES

4-25. Larger signal elements, up to platoon size, usually co-locate with their supported command post. The signal personnel assist in perimeter defense. The supported unit headquarters conducts the overall defense of the command post. The signal element coordinates closely with the supported unit.

## REMOTE SITES

4-26. Planners must coordinate for security and sustainment when deploying signal sites remotely from the supported unit. When a signal site does not co-locate with the supported headquarters, the signal element conducts site defense. They must be prepared to survive enemy air, artillery, and chemical, biological, radiological, and nuclear attack with little outside assistance. Because of their size and limited defensive capabilities, signal elements need assistance from the supported unit to defend against a large-scale assault.

## SMALL TEAMS

4-27. Small teams often operate from isolated positions, usually for retransmission. Teams should try to remain concealed and report enemy activity to higher headquarters. The teams conduct risk assessments at remote sites to determine the likelihood of mission success. Supported unit leaders must carefully track threats and move teams quickly when in danger.

## SIGNATURE REDUCTION

4-28. 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

4-29. Command posts require 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.

### Camouflage and Concealment

4-30. 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.

4-31. 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 a 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.

## Light Discipline

4-32. Excessive light makes tactical sites easy to locate at night. Signal site plans must actively seek to implement light discipline to minimize the chances of detection. During site setup, Soldiers should cover or blacken any reflective surfaces, such as bare metal surfaces or vehicle windshields. Minimize the use of flashlights or other electrical lights to prevent visual detection. Lit cigarettes and cigars are visible from great distances at night.

4-33. If Soldiers need more illumination than an image intensifier can provide in infrared mode during movement, they should use additional infrared light sources. The combination should provide the light needed with the least risk of enemy detection. When using infrared light, leaders must consider the enemy's night vision and infrared capabilities. For instance, an enemy with night vision capability can sense infrared light signals, and concentrate direct and indirect fire on a platoon using infrared light.

## ELECTROMAGNETIC

4-34. *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).

4-35. Commanders should consult with intelligence G-2 or S-2 and EW personnel to identify threat EW capabilities and intent to collect intelligence through the electromagnetic spectrum. Additionally, EW professionals must evaluate the effectiveness of friendly force emission control and recommend modifications or improvements. This process should take place before mission execution. Units should implement and exercise emission control plans before execution and conduct vulnerability analysis and assessments of friendly communications assets to understand the electromagnetic environment.

4-36. Employing aspects of emission control will help prevent enemy EW assets from discovering and attacking friendly locations. Electromagnetic protection is only effective when everyone in an organization understands its importance and can readily identify opportunities to implement protection activities (ATP 3-12.3).

4-37. Radio discipline is the most basic and effective emission control technique to protect against enemy EW. Radio discipline can take the form of limiting transmissions, antenna masking, and the use of low power. Additional techniques for emission control include—

- **Preplan messages before transmitting.** The radio operator should know what to say before beginning a transmission. Write out the message before beginning the transmission. This minimizes the number of pauses in the transmission and decreases transmission time. It also ensures the conciseness of the message.
- **Transmit quickly and precisely.** This is critical when the quality of communications is poor. This reduces the need to repeat a radio transmission. Unnecessary repetition increases transmission time and the enemy's opportunity to intercept U.S. transmissions and gain valuable information. When a transmission is necessary, the radio operator should speak in a clear, well-modulated voice, and use proper radiotelephone procedures.
- **Use equipment capable of data burst transmission.** This is one of the most significant advantages of tactical satellite communications systems. Soldiers use limited time for encoded messages on a digital entry device for transmission over satellite systems.
- **Use an alternate means of communication.** Soldiers use alternate means of communications, such as cable, wire, or messages to convey necessary directives and information.
- **Use brevity codes.** A brevity code is a code that provides no security, but which has as its sole purpose the shortening of messages rather than the concealment of their content. (Refer to ATP 1-02.1 for more information on brevity codes.)

4-38. When evaluating command post electromagnetic signatures, planners should consider concentrations of vehicles. Parking vehicles and aircraft away from command posts mitigates the concentrated electromagnetic signature. Planners should also consider installing antennas away from the command post to

enhance signature reduction. Operating antenna systems away from a command post requires planning for site security and defense.

4-39. G-6 or S-6 planners should collaborate with the cyber electromagnetic warfare officer during signal site planning and consider using electromagnetic masking and 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 transmissions from enemy electromagnetic warfare support and signals intelligence capabilities. Refer to ATP 3-12.3 for more information about electromagnetic masking.

4-40. A large number of antennas, electromagnetic emissions, and support towers are common in major command posts. If tactically feasible, units should use remote antennas to reduce the vulnerability of the command post to collateral damage if an enemy destroys the communications system. Radar reflective camouflage netting can help mask electromagnetic signature from the back and sides of directional antennas.

## **NOISE**

4-41. Noise discipline contributes to command post survivability. During site setup, soldiers should secure loose metal parts of signal assemblages to prevent them from making noise in the wind. The power generation equipment associated with signal equipment can generate significant noise. During site selection, signal leaders should consider measures to mask and diffuse the noise from electrical generators and environmental control equipment. Once the signal site is set up, leaders should restrict unnecessary vehicle and foot movement. Soldiers should limit outdoor talk and minimize radio use. When radio use is necessary, operators should turn the speaker volume to the lowest setting they can hear.

## **RADAR**

4-42. 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. When possible, Soldiers should emplace barbed wire and concertina wire to follow natural terrain features to reduce their radar signature.

## **INFRARED**

4-43. 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 signatures. Heat diffusers that disperse and vent vehicle exhaust away from the threat sensors are expedient means of thermal signature reduction.

## **Appendix A**

# **Attachments to Annex H**

Commanders and staffs use annex H (Signal) to describe how signal supports the concept of operations described in the base plan or order. The G-6 or S-6 develops annex H (Signal) using the five-paragraph attachment format from FM 6-0. This appendix provides templates for suggested appendixes and tabs to Annex H (Signal) of an operation plan or order.

### **APPENDIX 1—CONCEPT OF SIGNAL SUPPORT OVERLAY**

A-1. The concept of signal support includes necessary support tasks performed by non-signal personnel, such as quick reaction force, security, and casualty evacuation and describes how signal elements support the commander's intent and concept of operations, by phase, as described in the base plan or order.

A-2. The concept of signal support describes the templated locations of all command and control nodes—including command posts and retransmission sites—needed to support the concept of operations and describes the systems and capabilities residing at each of the command posts to enable communication to higher, subordinate, and adjacent units as required. It should also define the PACE plan as it is nested within the concept of signal support.

A-3. The concept of signal support defines triggers to transition command and control and technical channels across the various command posts throughout the operation. The concept of signal support establishes the priorities of support to units for each phase of the operation. Refer to Annex C (Operations) as required.

A-4. Signal elements and capabilities exist to meet commanders' information requirements and enable control of forces. The DODIN-A extends from the lowest tactical echelons to the highest levels of command. As a warfighting platform, the network enables integration of combined arms and all elements of combat power. Signal capabilities support command and control and enable strategic responsiveness, ultimately leading to a marked information advantage in the operational area.

### **TAB A—RETRANSMISSION TEAM MISSION CHECKLIST**

A-5. Radio retransmission extends single-channel radio networks to overcome obstacles and distance which are traditional limitations of frequency-modulated communications. Retransmission teams conduct team mission checks before all missions. The retransmission site uses two connected radios within the outer edges of at least two distant stations that are not within range of each other. The radios receive the signal from either of the distant stations and rebroadcast, or retransmission, so that the message is receivable by the distant station.

## APPENDIX 2—DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS

A-6. Appendix 2 of annex H of the Army operation order, describes how DODIN operations (including cybersecurity and COMSEC) support each phase of the operation in the base plan or order. Examples of support include validation of the following:

- WIN-T.
- Mission command information systems.
- Lower tier tactical internet.
- Coordination with subordinate elements.

### TAB A—CYBERSECURITY INCIDENT BATTLE DRILL

A-7. Personnel experiencing network abnormalities should begin conducting the cybersecurity incident battle drill. Examples of abnormal activities would include slow network, internet browser pop-ups, home page redirection, and text messages from unknown personnel. See table A-1 below provides an example cybersecurity battle drill.

**Table A-1. Cybersecurity incident battle drill**

<b>Tab A to Appendix 2- Cybersecurity Incident Battle Drill</b>	
Malicious software detected.	Remove network cable from computer
Computers experiencing slow internet connectivity.	Notify network operations.
Identifies strange new alerts.	Notify network operations.
New files on computer.	Notify network operations.
Unusual system activity.	Notify network operations.
Request from unknown individual requesting network access.	Notify network operations.
Change in computer wallpaper or pop-up notifications.	Notify network operations.

### TAB B—CYBERSECURITY INCIDENT REPORT

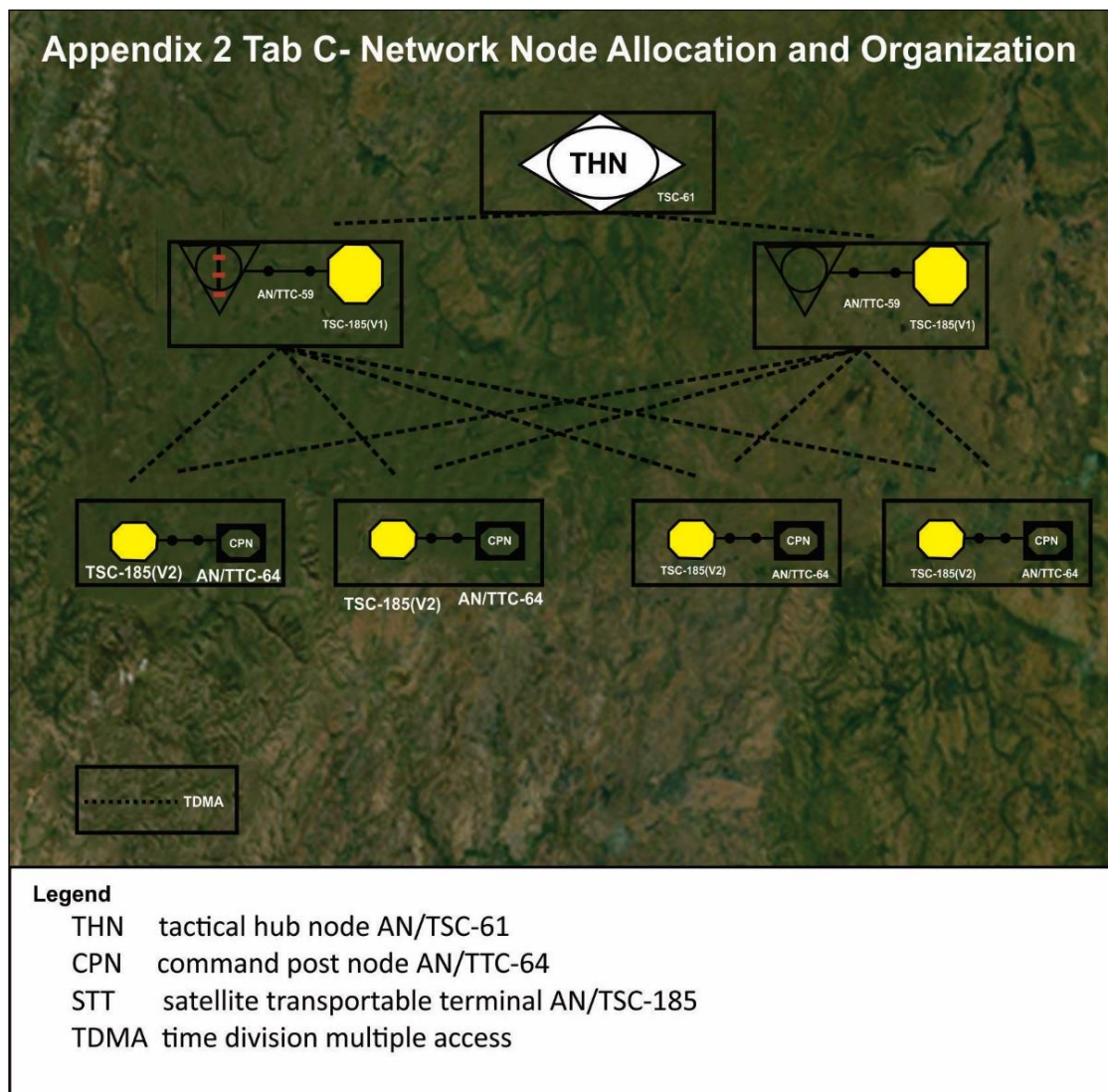
A-8. Personnel experiencing cybersecurity incidents should complete a cyber incident report. Users will provide verbal notification to the chain of command and submit an informal report before submitting a cyber incident report to the G-6 or S-6.

A-9. Users experiencing a cybersecurity incident will provide the suggested minimum information—

- Reporter's name.
- Reporter's phone or email.
- Type of incident.
- Location of incident.
- Date of discovery
- Time of discover
- Circumstances surrounding incident.

A-10. The network node allocation and organization tab provides a graphic depiction of the elements' network assets. See figure A-1 below. This graphic should be seen in color for complete clarity.

**TAB C—NETWORK NODE ALLOCATION AND ORGANIZATION**



**Figure A-1. Tab C to Appendix 2—Network node allocation and organization**

**TAB D—NETWORK OUTAGE PROCEDURES AND REPORT**

A-11. Network outage procedures include the immediate notification to the G-6 or S-6 section. Upon loss of communications capability, Network Management will notify G-6 or S-6 of the outage, including time and system(s) affected.

- Units and command posts will rely on the published PACE plan as the G-6 develops a contingency plan to continue operations by alternate means.
- Signal support personnel begin work to restore lost network capability.
- NETOPS takes steps to continue operations throughout the outage, notifies stations of the situation, and of any contingency plan(s) to transfer to an alternate net or transport system.
- •G-6 provides an hourly SITREP to G-3 while net is out of service.
- •Outages lost due to jamming is reported to the CEMA section, spectrum manager, and protection cell for potential counterjamming and exploitation for targeting.
- •Upon network restoration, G-3, in conjunction with the network management team, coordinates controlled transfer and restoration for each net.
- •G-6 reports reason for outage to G-3.

**TAB E—SCHEME OF NETWORK MONITORING**

A-12. Network monitoring helps network and systems administrators identify possible issues before they affect the established network. Continuous monitoring helps to develop and maintain a high performing network with minimal downtime.

A-13. Network monitoring supports the following network management activities:

- **Fault Management.** The process of recognizing, isolating, and resolving an incident, including the identification of potential problems.  
**Configuration Management.** The collection and storage of configuration details from various network devices including change management.
- **Enterprise Administration.** The administration of services on the network.
- **Performance Management.** The parameters associated with performance management. This may include metrics with respect to throughput, packet loss, response times, and usage.
- **Security.** The process of controlling access to resources in the network, which includes data as well as configurations and protecting users from unauthorized users.

A-14. Monitoring systems should be comprehensive and cover every aspect of the deployed capability. At a minimum, the following network and system elements should be monitored:

- **Availability.** Continuous monitoring of resources and services to ensure that the node or service is available to meet requirements.
- **Interfaces.** Interface monitoring will help identify possible network issues. It may include monitoring for errors, packet loss, discards, and utilization limits.
- **Disk monitoring.** This may include—
  - Read and write performance.
  - Space usage.
  - Disk errors.
  - Large file statistics.
  - Free space monitoring.
- **Hardware.** Hardware health monitoring should capture central processing unit usage, fan speed, memory usage, hard drive usage, temperature, and status of the power supply.
- **Application Performance.** Monitors, analyses, and summarizes usage according to individual applications, locations, and types of user.
- **Network Discovery.** Enables visualization of the network to identify anomalies of the planned network and assist in the change management process.

A-15. Network and system monitoring tools typically include—



- Internet Control Message Protocol.
- Secure Shell.
- Simple Network Management Protocol.
- Windows Management Instrumentation.
- Internet Protocol Service Level Agreement.
- NetFlow.

## **APPENDIX 3—NETWORK TRANSPORT AND INFORMATION SERVICES**

A-16. The Network Transport and Information services appendix describes routing and movement of voice, video, and data network traffic using primary and alternate routes while supporting the commander's intent and concept of operations described in the base plan or order. This appendix establishes the priorities of support to units for each phase of the operation and provides a detailed network diagram including the internet protocol scheme of the network.

### **TAB A—LINE OF SIGHT ANALYSIS**

A-17. Spectrum managers create the line of sight analysis using spectrum management tools. They calculate the propagation prediction values for the maximum usable frequency, the frequency of optimum transmission, and the lowest usable frequency based on the time of day between a transmitting and receiving location.

### **TAB B—HIGH FREQUENCY RADIO NETWORK DIAGRAM**

A-18. Spectrum managers create the high frequency analysis network diagram to calculate the high frequency propagation prediction values for the maximum usable frequency, the frequency of optimum transmission, and the lowest usable frequency based on the time of day between a transmitting and receiving location.

## TAB C—VOICE, VIDEO, AND DATA LOGICAL NETWORK DIAGRAMS

A-19. The voice, video, and data logical network diagram depict the planned network unit connectivity. Network planners create the voice and video data logical network diagrams, and they are typically approved by the commander. Figure A-2 depicts the logical network diagram for voice, video, and data. This graphic should be seen in color for complete clarity.

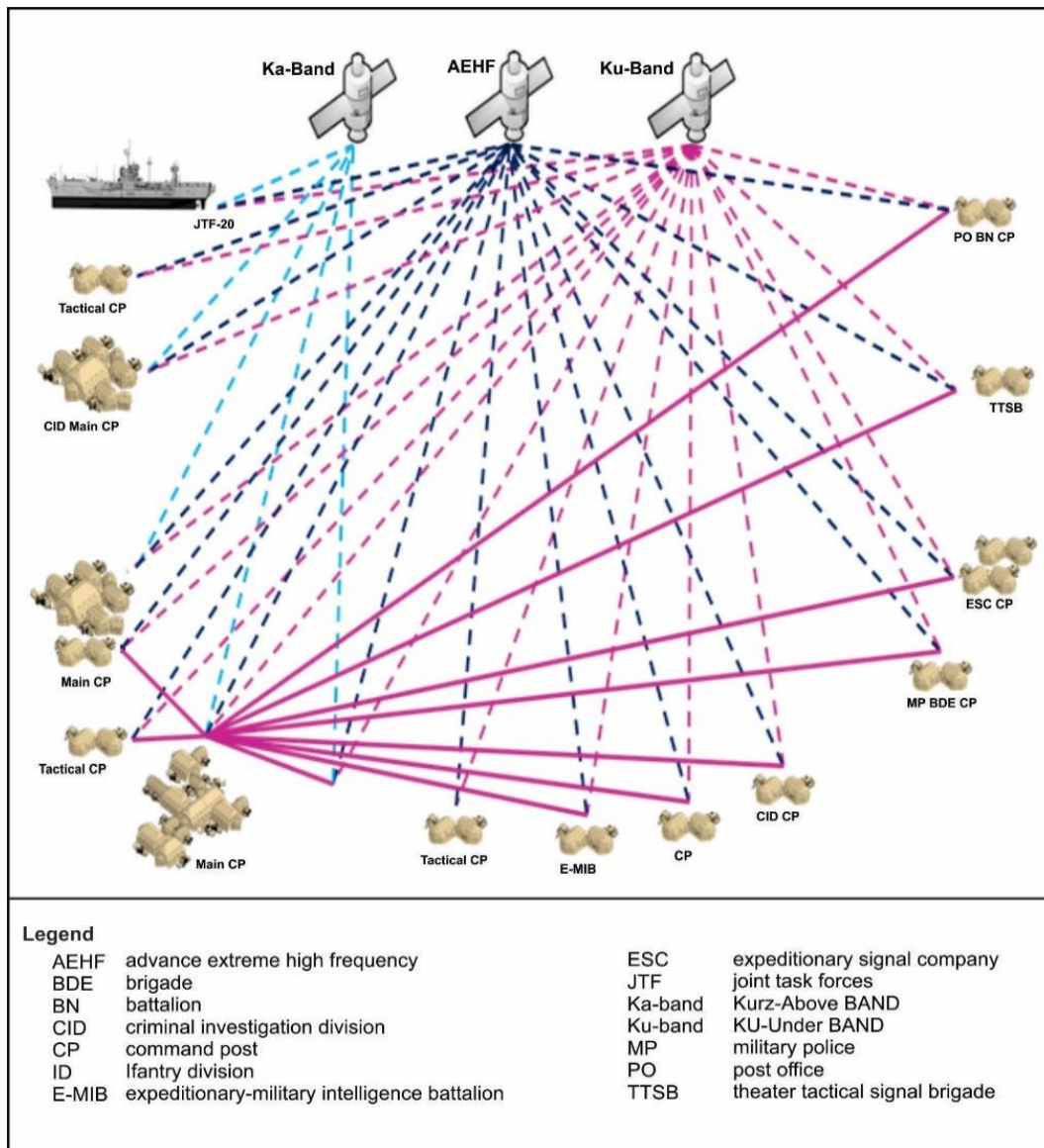


Figure A-2. Example Tab C to Appendix 3—Voice, video, and data logical network diagram

## TAB D—VOICE OVER INTERNET PROTOCOL PHONE BOOK

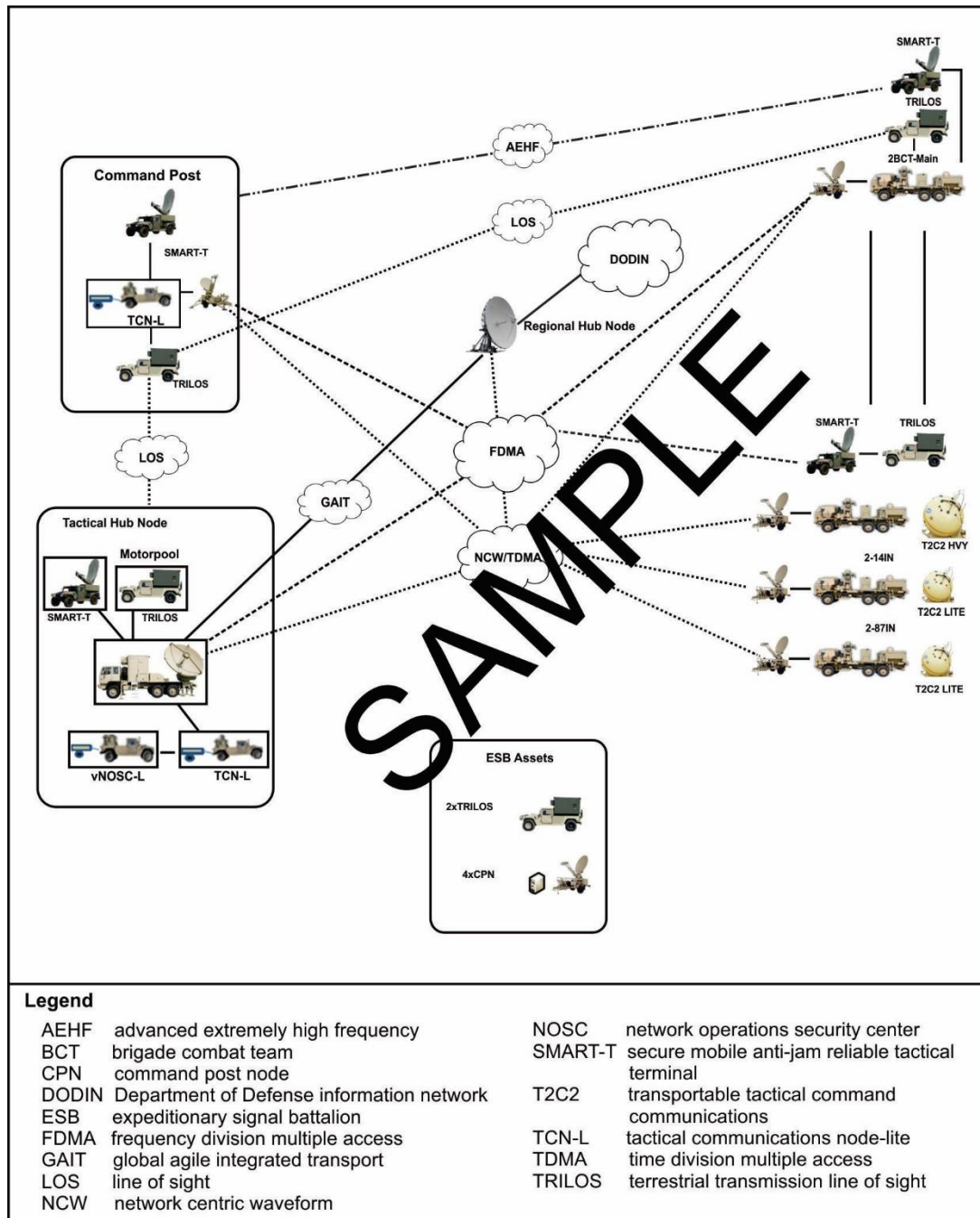
A-20. Units create the voice over internet protocol phone book for distribution to all users. The phone book distribution can be printed or electronic. Units include phone numbers for all sections. Table A-2 depicts a sample voice over internet protocol phone book.

**Table A-2. Voice over internet protocol phone book.**

Battalion Command Post Node 3	
Commander	795-6301
Executive Officer	795-6302
Command Sergeant Major	795-6303
S-1	795-6304
S-2	795-6304
S-3	795-6305

### TABLE E—UPPER TIER SATELLITE TRANSMISSION DIAGRAM

A-21. The upper tier satellite transmission diagram depicts the proposed satellite communications network. This diagram should include element locations, equipment node names, and satellite coverage data. Figure A-3 illustrates an upper tier satellite transmission diagram.



**Figure A-3. Sample Tab E to Appendix 3—Upper tier satellite transmission diagram**

## **TAB F—COALITION FORCES NETWORK DIAGRAM AND FOREIGN DISCLOSURE GUIDANCE**

A-22. Coalition networks connect partner nation-owned networks to the core of the DODIN. AR 380-10, Foreign Disclosure and Contacts with Foreign Representatives, outlines procedures for the disclosure of information to international personnel as well as procedures for hosting international visits. Individuals must coordinate the disclosure of classified information to the organizational security manager who will pass the requests to the S-2 or G-2 Foreign Disclosure Officer. The G-2 must coordinate classified information disclosure with the original classification authority.

## **TAB G—SATELLITE ACCESS AUTHORIZATIONS AND GATEWAY ACCESS AUTHORIZATIONS**

A-23. Satellite access authorizations and gateway access authorizations enable access to the DOD satellite network. Planners should be prepared to provide—

- Terminal type/nomenclature.
- Certification number
- Geographical location (city, country).
- Latitude of location (north or south) (degrees:minutes:seconds).
- Longitude of location (east or west) (degrees:minutes:seconds).
- Terminal look angle restrictions (yes/no).
- Antenna diameter (in meters).
- Antenna manufacturer.
- Antenna model number.
- Currently supporting existing satellite mission.
  - Indicate satellite for existing transmit or receive requirements:
  - Transmit carrier polarization.
  - Receive carrier polarization.
- Antenna polarization capability.
- Feed assembly (2-port, 4-port).
- Feed assembly options (co-polarized, cross-polarized).
- Antenna platform (fixed, mobile, or transportable).
- Earth terminal frequency band.
- Earth terminal transmit frequency range.
- Earth terminal receive frequency range.
- Upconverter tuning resolution.
- Upconverter bandwidth.
- Downconverter tuning resolution.
- Downconverter bandwidth.
- Automatic power control capability.
- Automatic power control level (in decibels).
- Auto tracking (yes or no).
- Saturated effective isotropic radiated power.
- Linear effective isotropic radiated power.

**TAB H—RETRANSMISSION NETWORK DIAGRAM**

A-24. The retransmission team's network diagram provides an overview of the proposed location and equipment. Planning the retransmission network is critical, as teams are often remotely located. Figure A-4 depicts a retransmission network diagram.

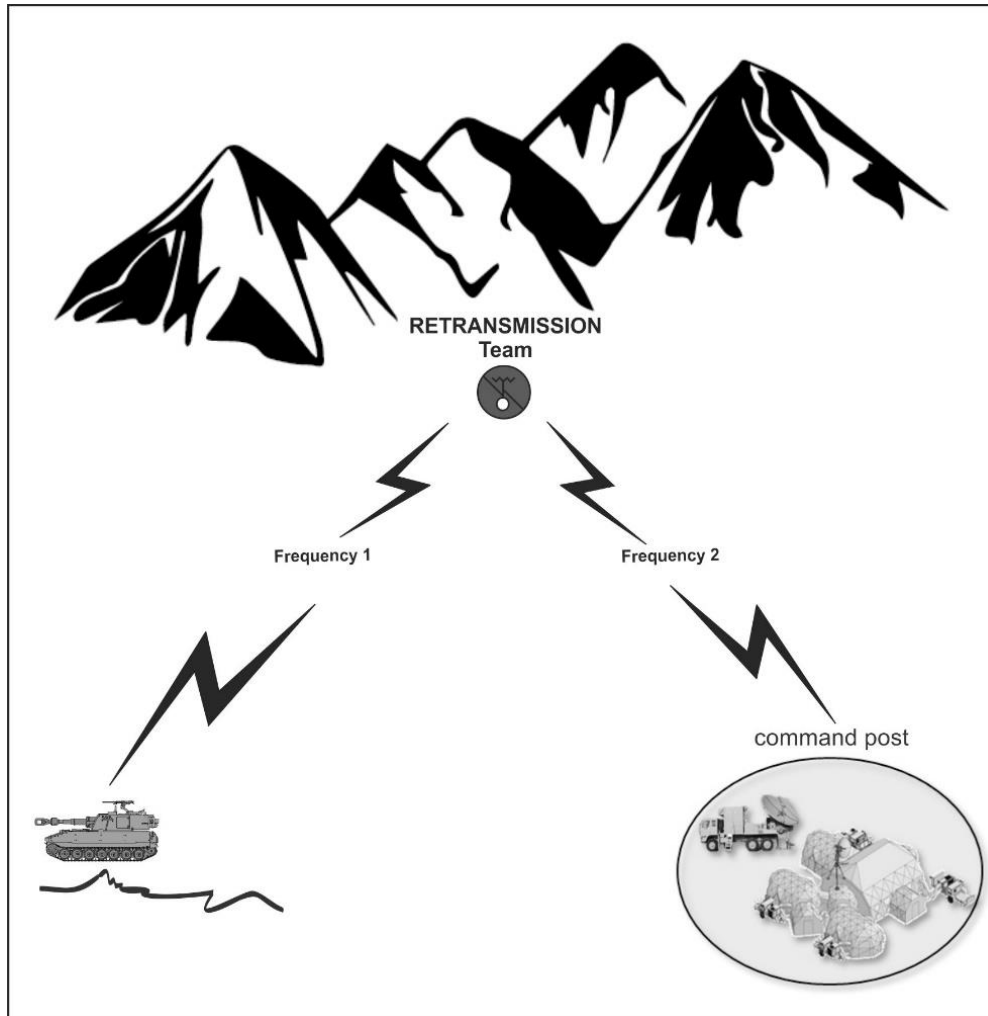


Figure A-4. Tab B—Retransmission network diagram

# **TAB I—MISSION COMMAND INFORMATION SYSTEMS ALLOCATION AND INTERCONNECTIONS (BATTLE COMMAND COMMON SERVER AND TACTICAL SERVER INFRASTRUCTURE CONFIGURATIONS)**

A-25. The mission command information systems allocation and interconnections example provides a depiction of the mission command systems availability. Commanders use this diagram for quick glance updates on the system status. Figure A-5 shows a sample of mission command information systems allocation and interconnections.

Mission Command Information Systems Allocation and Interconnections										
	SIPRNET	NIPRNET	Voice over IP	E-mail	ABCS	Chat	FM	JCR	TACSAT	Cell
Main Command Post										
Tactical Command Post										
Main Command Post B			no service provided			no service provided				
Tactical Command Post B										
Field Artillery A										
Field Artillery B										
Sustainment Company	no service provided									
Cavalry A										
Cavalry B										

**Legend**

ABCS Army Battle Command System

FM frequency modulation

JCR joint capabilities release

IP Internet protocol

NIPRNET Non-classified Internet Protocol Router Network

SIPRNET SECRET Internet Protocol Router Network

TACSAT tactical satellite

system allocated and connected

no system allocation and connections

**Figure A-5. Sample Tab I—Mission command information systems allocation and interconnections**

## **TAB J—TACTICAL SATELLITE NETWORK DIAGRAM**

A-26. The tactical satellite network diagram provides an overview of the satellite network. Signal planners design the tactical satellite network to meet the commander's objectives.

A-27. The commander's objectives create requirements that dictate the tactical satellite network. Planners use the commander's intent to design the tactical satellite network. Objectives include—

- Interoperability.
- Connectivity—
  - Coverage.
  - Capacity.
  - Protection.
- Cybersecurity.
- Operational management.
- Operational suitability.

**TAB K—DIGITAL FIRES DIAGRAM**

A-28. The digital fires diagram depicts the planned digital fires in an area of operations. The digital fires diagram provides an overview of communications networks that connect the fires support control equipment. Fires support command and control equipment provides the ability to integrate and target lethal or non-lethal fires and effects. Fires support command and control equipment also provide the capability to visualize effects, increase situational awareness, and facilitate collaboration among commanders and fires staff elements. Advanced Field Artillery Tactical Data System is the Army's primary fire support command and control system. For further information on fire support, refer to FM 3-09.

**APPENDIX 4—SPECTRUM MANAGEMENT OPERATIONS**

A-29. Spectrum management operations enable cyberspace electromagnetic activities by ensuring access and deconfliction for the Army's use of the electromagnetic spectrum. Planning, integration, and synchronization of the interrelated actions support the overall mission (FM 6-02). Spectrum management operations activities begin upon receipt of the warning order. Spectrum managers collaborate with the G-6 or S-6 to develop the Annex H (Signal) and its appendixes and tabs. Table A-3 depicts a sample emitter list for an area of operations.

**Table A-3. Sample Appendix 4—Spectrum management operations emitter list**

System	Emitter	Model	Start Frequency	Stop Frequency	Minimum Power	Maximum Power	Channel Bandwidth	Data Rate
SMART-T	SMART-T	AN/TSC-154	20200 MHz (down)	21200 MHz (down)	classified	classified	2 Ghz	75-2400 bps
SMART-T	SMART-T	AN/TSC-154	43000 MHz (up)	45000 MHz (up)	classified	classified	2 Ghz	4.8-1544kbps
SINGGARS	SINGGARS SIP/RT-1523	AN/VRC-87	30 MHz	88 MHz	500 mw	4w	25 MHz	16 kbps
SINGGARS	SINGGARS SIP/RT-1523	AN/VRC-88	30 MHz	88 MHz	500 mw	4w	25 MHz	16 kbps
SINGGARS	SINGGARS SIP/RT-1523	AN/VRC-89	30 MHz	88 MHz	500 mw	4w	25 MHz	16 kbps
SINGGARS	SINGGARS SIP/RT-1523	AN/VRC-90	30 MHz	88 MHz	500 mw	4w	25 MHz	16 kbps
<b>Legend</b> bps            bytes per second            SMART-T    secure, mobile, anti-jam, reliable tactical-terminal GHz           gigahertz                            mw            milliwatt Kbs           kilobytes per second                   MHz           megahertz SINGGARS   single-channel ground and airborne radio system            w            watt								

**TAB A—SIGNAL OPERATING INSTRUCTIONS AND FREQUENCY ALLOCATION (COMMUNICATIONS CARD AND TACTICAL RADIOS).**

A-30. Signal operating instructions provide network identification call signs, call words, frequency assignments, signs, and countersigns for radio nets, as well as pyrotechnic and smoke signals dictionaries. Signal operating instructions also provide call sign information, crypto change over times, and other information. Spectrum managers typically create the signal operating instructions in collaboration with the S-6 or G-6 personnel.



## **TAB B—SIGNAL OPERATING INSTRUCTIONS (LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL DATA INTERCHANGE FORMAT)**

A-31. The Lightweight Directory Access Protocol Data Interchange Format is the sourcing document for all assigned unit organic IP space. Automated information systems use their assigned IP space as identified in the Lightweight Directory Access Protocol Data Interchange Format to integrate automated information systems.

A-32. Planning IP addresses entails forecasting IP address capacity requirements. This ensures IP addresses are available and provides room for growth. Planners coordinate IP address advertisement and de-advertisement with the local installation and the regional or tactical hub node to avoid dual advertisement.

## **TAB C—JOINT RESTRICTED FREQUENCY LIST**

A-33. The joint restricted frequency list defines those frequencies that are protected from specific uses. The list is not a static product as it may change as appropriate for the mission.

- **Taboo frequencies:** These frequencies include friendly international distress, stop buzzer, safety, and controller frequencies. They are generally long-standing as well as time-oriented. For example, as the combat or exercise situation changes, the restriction must be removed.
- **Protected frequencies:** These are frequencies used for a particular operation. Units identify protected frequencies to prevent inadvertently jammed by friendly forces, while directing active EW operations against hostile forces. These frequencies are of such critical importance that jamming should be restricted unless necessary or until coordination with the using unit is made. They are generally time-oriented may change with the tactical situation, and must be updated periodically. An example of a protected frequency would be the command net of a maneuver force engaged in the fight.
- **Guarded frequencies:** Enemy frequencies that are currently being exploited for combat information and intelligence. A guarded frequency is time oriented in that the list changes as the enemy assumes different combat postures. These frequencies may be jammed after the commander has weighed the potential operational gain against the loss of technical information. Refer to ATP 6-02.70 for more information on the joint restricted frequency list.

## **TAB D—JOINT SPECTRUM INTERFERENCE RESOLUTION REPORT FORMAT AND PROCEDURES**

A-34. 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. Operators encountering EMI use the JSIR-Online. The JSIR-Online portal is located on the SECRET Internet Protocol Router Network. Unit standard operating procedures may also require JSIR approval from the chain of command using the JSIR format. The report preparer provides a copy of the completed report to the CEWO, spectrum manager, and G-6 or S-6 staff.

## **TAB E—GUARDED FREQUENCY LIST**

A-35. Refer to paragraph A-32 for a description of guarded frequencies.

# **APPENDIX 5—COMMUNICATIONS SECURITY**

## **TAB A TO APPENDIX 5, COMMUNICATIONS SECURITY CALLOUT MESSAGE**

A-36. The key management infrastructure operating account manager coordinates key requirements and produces a COMSEC callout message to identify encryption keys for joint, theater Army, corps, or division use. As the theater Army and subordinate units identify network requirements, they compile a master network list.

**TAB B TO APPENDIX 5, KNOWN SUPERSESSION DATES**

A-37. Known supersession dates refer to the cryptographic period and expiration date assigned to encryption keying material. The unit signal operating instructions provide the known supersession dates. The signal operating instruction directs users to advance to a new segment or date.

A-38. Zeroizing is a method of destroying superseded encryption keys. Users destroy or zeroize superseded encryption keys when they are no longer needed, upon supersession of the keying material, or when directed by the controlling authority.

**TAB C—COMMUNICATIONS SECURITY COMPROMISE PROCEDURES**

A-39. A COMSEC compromise occurs when COMSEC material is irretrievable or lost, information has been disclosed to unauthorized individuals, or a violation of the security policy for a system in which unauthorized intentional or unintentional disclosure, modification, or destruction may have occurred.

A-40. Users experiencing compromised communications security should immediately stop transmission on the compromised system and notify the G-6 or S-6. At a minimum, provide the following information to the G-6 or S-6—

- Unit experiencing compromise.
- Equipment type and nomenclature.
- Crypto segment or crypto period.
- Time and location of compromise.

## **Appendix B**

# **Equipment Cut Sheets**

This appendix displays sample cut sheet formats and brief descriptions for various tactical signal assemblages. The purpose of this appendix is to aid planners in the execution of DODIN-A planning. The Cyber Lessons Learned website contains a large repository of signal, cyberspace and EW information.

### **JOINT NETWORK NODE**

B-1. The Joint Network Node uses satellite communications and high bandwidth 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 backbone connection. The backbone connection is the frequency division multiple access link that allows connectivity to the DODIN-A while providing access to Defense Information Systems Network services for the Joint Network Node and all associated command post nodes in the wide-area network.

B-2. The Joint Network Node connects to the tactical hub node or regional hub node using Ku band commercial satellite communications or Ka-band military satellite communications for gateway access to the DODIN and Defense Information Systems Network services. The Joint Network Node connects users to SIPRNET, NIPRNET, secure and nonsecure analog phones, secure voice-over Internet Protocol phones, and battlefield video teleconferencing. The Joint Network Node uses either the Satellite Transportable Terminal or the high capacity line of sight radio system for its primary network transport. It can also use a Phoenix satellite communications terminal or SMART-T as alternate network transport. Table B-1 on page B-2 provides an example of Joint Network Node settings when connecting to the Satellite Transportable Terminal.

Table B-1. Example Joint Network Node cut sheet

<b>Settings</b>	<b>Joint Network Node Fiber</b>	<b>Satellite Transportable Terminal</b>
Mode	Fiber Optic	Fiber Optic
INPUT	NRZ	NRZ
Rate	Data Rate Provided	Data Rate Provided
Mode	EIA530A	EIA530A
NRZ Configuration	DCE/external	DTE/internal
Clock Source	EXT/5	Fiber
Clock Edge	Normal	Normal
Data Polarity	Normal	Normal
Test Pattern	Zeros	Zeros
Test Mode	OFF	OFF
LOOP	OFF	OFF
Error Rate	Disabled Unless in Test Mode	Disabled Unless in Test Mode
Error Count	Disabled Unless in Test Mode	Disabled Unless in Test Mode
<b>Legend:</b> DCE      data circuit terminating equipment DTE      data terminal equipment EIA      electronic industries alliance NRZ      non-return zero		

## TACTICAL FLEXIBLE MULTIPLEXER

B-3. Table B-2 is an example of the tactical flexible multiplexer settings.

**Table B-2. Tactical flexible multiplexer settings**

Parameters	Settings
Multiplex	
Timing	External_Analog_10 Megahertz
Framer	off
MTG_select	disabled
Multiplex Internal Loopback	off
Multiplex_External Loopback	off
CUT3_Int Loopback	off
DS3_Ext Loopback	off
Self-test	off
PORT	
Rate	
Shutdown	No shutdown
Invert – input_clock	on
Invert – input_data	on
Invert – output_clock	off
Invert – output_data	on
Loopback	off

## COMMAND POST NODE

B-4. The Command Post Node establishes a small communications node that extends limited Defense Information Systems Network services, including SIPRNET, NIPRNET, secret and non-classified voice over internet protocol, and video teleconferencing services. The Command Post Node uses the network centric waveform, to provide users with DODIN-A connectivity and access to Defense Information Systems Network services. The Command Post Node connects to the DODIN-A through either satellite communications or high capacity line of sight transport to the Joint Network Node, or satellite communications to the tactical hub node. Table B-3 provides a sample Command Post Node cut sheet.

**Table B-3. Sample Command Post Node cut sheet**

Command Post Node cut sheet	
Terminal Identifier	<b>Command Post Node</b>
Terminal Type/Nomenclature	AN/TSC-167(V2)M
Federal Communications Commission License	Varies
Geographical Location (City, Country)	Varies
Latitude of Location	Varies
Longitude of Location	Varies
Terminal Look Angle Restrictions	NO
Antenna Diameter (meters)	2.4M
Antenna Manufacturer	VERTEX RSI
Antenna Model Number	2.4M SM-LT Multi Band
Currently Supporting Existing Mission	NO
Transmit Carrier(s) Polarization	Left Hand Circular Polarization
Receive Carrier(s) Polarization	Left Hand Circular Polarization
Antenna Polarization Capability	Linear
Feed Assembly	2-port
Feed Assembly Options (Polarized, Cross-Polarized)	Cross-Polarized
Antenna Platform (Fixed, Mobile, Transportable)	Transportable
Earth Terminal Frequency Band	KU
Earth Terminal Transmit Frequency Range	14-14.5 GHZ
Earth Terminal Receive Frequency Range	10.95-12.75 GHz
Upconverter Tuning Resolution	1 KHz
Upconverter Bandwidth	36 MHz
Downconverter Tuning Resolution	1 KHz
Downconverter Bandwidth	76 MHz
Automatic Power Control Capability	No
Automatic Power Control Level	N/A
Auto Tracking (Yes/No)	Yes
Nominal Gain-to-Noise-Temperature	26.6 decibel watt
Saturated	69.7 decibel watt
<b>Legend</b> KHz kilohertz GHz gigahertz MHz megahertz	

## TACTICAL COMMUNICATIONS NODE

B-5. The Tactical Communications Node is the main node type in WIN-T increment 2. The Tactical Communications Node provides at-the-halt and on-the-move high capacity C band ground-to-ground communications and Ka- or Ku-band (swappable) satellite communications. The Tactical Communications Node provides connection to Ethernet switches, supporting ports for user equipment phones, computers, or video teleconferencing. Each Tactical Communications Node is equipped with a Modular Communications Node-Basic that provides a 48-port Ethernet switch and a 24-port analog phone gateway. Table B-4 provides a sample Tactical Communications Node cut sheet.

**Table B-4. Sample Tactical Communications Node cut sheet**

Tactical Communications Node Cut Sheet	
Terminal Identifier	Tactical Communication Node
Terminal Type/Nomenclature	AN/MSC-82
Certification Federal Communications Commission License	Varies
Geographical Location (City, Country)	Varies
Latitude of Location	Varies
Longitude of Location	Varies
Terminal Look Angle Restrictions	.508m
Antenna Diameter (meters)	2.4m
Antenna Manufacturer	General Dynamics
Antenna Model Number	GD20-20
Currently Supporting Existing Mission	N/A
Transmit Carrier(s) Polarization	Select
Receive Carrier(s) Polarization	Select
Antenna Polarization Capability	Linear
Feed Assembly	2-port
Feed Assembly Options Polarized, Cross-Polarized	Cross-Polarized
Antenna Platform (Fixed Mobile Transportable)	Transportable
Earth Terminal Frequency Band	KU
Earth Terminal Frequency Range (Gigahertz)	13.75-14.35
Earth Terminal Receive Frequency Range (Gigahertz)	10.95-12.75
Upconverter Tuning Resolution	1 Kilohertz
Upconverter Bandwidth	500 Megahertz
Downconverter Tuning Resolution	1 Kilohertz
Downconverter Bandwidth	1800 Megahertz
Automatic Power Control Capability	No
Automatic Power Control Level	N/A
Auto Tracking (Yes/No)	Yes
Nominal Gain-to-Noise-Temperature	12.5dBi/K
Saturated	47dBW
Linear Effective Isotropic Radiated Power	45dBW
<b>Legend</b> dBi/K    decibels relative to isotropic in kilowatts dBW    decibel watt	

## POINT OF PRESENCE

B-6. A point of presence provides access to Defense Information Systems Network services for selected users at the battalion, brigade, and division. The point of presence supports high-throughput line of sight and satellite communications network transport. The point of presence is general-purpose user operated; it does not require dedicated manning by signal Soldiers. It operates either at-the-halt or on-the-move, but is mainly used on-the-move. The point of presence is mountable in a variety of command vehicles. The point of presence provides data and voice network access for reach between brigade combat teams, and reachback communications to the division.

B-7. When operating at-the-halt, the point of presence can provide access for wired IP data terminals or SIPRNET voice over internet protocol phones. When operating on-the-move, it provides the same capabilities to users on-board the vehicle. Network planners configure point of presence components before deployment. The network management subsystem can dynamically update subsequent configurations over-the-air. Table B-5 provides a sample point of presence cut sheet.

**Table B-5. Sample Point of Presence cut sheet**

Point of Presence cut sheet			
Satellite Configuration		Beam Configuration	
Satellite Name:	SES1	Beam Name:	1
Orbital Location:	101 W	Uplink Polarity	Vertical Linear
SVOW Offset Frequency:	0	Downlink Polarity	Horizontal Linear
PIN Select:	PN Code Set 1	Band:	Ku
Fan-n GTs Derated	Unchecked	Uplink Center Frequency:	SAA MHz
Beacon Frequency	11.701 GHz	Downlink Frequency:	SAA MHz
		Uplink Spreading Enable:	checked
System Configuration		Downlink Spreading Enable:	unchecked
Latitude		Bandwidth:	3 MHz
Longitude		CROW Slots:	1
BUC Lo Frequency (kHz):	12800000	Spreading:	BPSK-2
LNB LO Frequency (kHz)	107500000	Most Disadvantaged Configuration	11
Rx Attenuator (K):	200	G/T:	41
RX Gain (dB):	59	EIRP:	0
Antenna Type:	Circular	Contour Offset EIRP:	0
Aperture	<56 Inch	Contour Offset G/T:	0
Bandwidth Segment Configuration	1	Contour Offset SFD:	0
Identification number:	1		
Uplink Beam	1		
Downlink Beam:	14479 MHz	Gain of this Bandwidth Segment	
Uplink Center Frequency	12179 MHz	Saturated Flux Density:	
Downlink Center Bandwidth:	3 MHz	Input / Output Backoff:	
Beam Segment Bandwidth:	11	Max Terminal EIRP	
EIRP:		Transfer Gain (dB)	



Table B-5. Sample Point of Presence cut sheet (continued)

Preferred Gain State Settings		Network centric waveform configuration	
Terminal Minimum EIRP:	0	Node Name:	POP=7950100
Terminal Maximum EIRP:	94	Transmit Chain Gain Factor:	82
Terminal Minimum GT:	0	Receive Sensitivity – G/T”	13
Terminal Maximum GT:	27	Max Terminal EIRP:	46
<b>IP Address Configuration</b>		Min Terminal EIRP:	6
CDU Ipv4 Address:	192.0.1.3	Contact EIRP:	46
CDU Ipv4 Address:	Not Applicable	RFOW Speed Factor:	BPSK-1
Data Ipv4 Subnet Address:	10.126.2.41	RFOW B/W Segment ID:	1
Data Ipv4 Subnet mask	255.255.0.0	Contour Offset EIRP:	1.2
Data Gateway	192.0.1.254	Contour Offset G/T	2.1
		Contour Offset SFD:	2.1
<b>Frequency reference options</b>		Terminal Type:	NM
Ext VDC Tx	No	Hub Assist	Checked/Unchecked
+18V Tx	No	Auto NC Handover	Unchecked
10 MHz Tx	Yes		
10 MHz Rx	No		
<b>Advance</b>			
Modulator(s)	2		
<b>QOS</b>	42 entries		
<b>Legend</b> <div style="display: flex; flex-wrap: wrap;"> <div style="flex: 50%;"> BPSK    binary phase shift keying  BUC    block up converter  B/W    bandwidth  CDU    computer data unit  CROW   control reference order wire  DB    decibel  EB/NO   energy per bit to noise power spectral density ratio  EIRP   effective isotropic radiated power  EXT    external  Ghz    gigahertz  GT    gain to noise temperature  IPv4   internet protocol version 4  K    kelvin  LO    local oscillator </div> <div style="flex: 50%;"> LNB    low noise block down converter  Mhz    megahertz  NC    network control  NM    network member  PIN    personal identification number  POP    point of presence  QOS    quality of service  RFOW   reference forward order wire  RX    receive  SAA    satellite access authorization  SFD    saturation flux density  SVOW   secure voice order wire  TX    transmit  V    voltage  VDCTX   voltage direct current </div> </div>			

## SATELLITE TRANSPORTABLE TERMINAL

B-8. The satellite transportable terminal provides beyond line-of-sight network transport for the Tactical Communications Node, Joint Network Node, and Command Post Node and operates at-the-halt only. Table B-6 provides sample settings when configuring the satellite transportable terminal for frequency division multiple access.

**Table B-6. Sample Satellite Transportable Terminal cut sheet**

Satellite Tactical Terminal Cut Sheet	
NETWORK SPECTRUM	CLOSED NET
STRAP CODE	000
FREQUENCY	[Transmission frequency from satellite access authorization]
POWER	-18
CARRIER	ON
SPECTRUM	NORMAL
MODULATION	[see satellite access authorization]
INTERNAL FORWARD CORRECTION	[see satellite access authorization]
DIFFERENTIAL CODING	DISABLED
SCRAMBLE SELECT	
SCRAMBLE CONTROL	ENABLED
SATELLITE FRAMING	NONE
DATA POLARITY	INVERT NONE
REED-SOLOMON	DISABLE
REED-SOLOMON RATE	219201
Data Modulation	
NETWORK SPECIFICATION	CLOSED NET
STRAP CODE	
FREQUENCY	
SPECTRUM	NORMAL
MODULATION	[see satellite access authorization]
SPECIAL MASK	INTELSAT 0.35
SWEEP RANGE	+/-25
SWEEP DELAY	000.0
FAST ACQUISITION	ENABLE
EB/NO ALARM	1 decibel THRESHOLD
DATA RATE	[see satellite access authorization]
INTERNAL FORWARD CORRECTION	[see satellite access authorization]
DIFFERENTIAL CODING	DISABLED
SCRAMBLE SELECTION	

## PHOENIX TERMINAL

B-9. Phoenix ground satellite terminals enable expeditionary signal battalions to provide large division and corps headquarters with high-bandwidth network communications and high capacity, inter- and intra-theater range extension for networked command and control information. Planners use the Phoenix terminal for high-throughput missions, which include unmanned air system feeds, video teleconferencing, and large numbers of subscribers and computers on the network. Table B-7 provides a sample of a Phoenix cut sheet.

**Table B-7. Sample Phoenix terminal cut sheet**

Phoenix Cut Sheet	
Terminal Identifier	Phoenix
Terminal Type/Nomenclature	AT/TSC-156
Certification Federal Communications Commission License	Varies
Geographical Location (City, County)	Varies
Latitude of Location	Varies
Longitude of Location	Varies
Terminal Look Angle Restrictions	NO
Antenna Diameter (meters)	2.4M
Antenna Manufacture	L3
Antenna Model Number	2.4 MVO Vertex
Currently Support Existing Mission	NO
Transmit Carrier(s) Polarization	Select
Receive Carrier(s) Polarization	Select
Feed Assembly	Select
Feed Assembly Option (Polarized, Cross-Polarized)	Linear
Antenna Platform (Fixed, Mobile, Transportable)	2-port
Antenna Platform (Fixed, Mobile, Transport	Adjustable
Earth Terminal Frequency Band	Transportable
Earth Terminal Transmit Frequency Range	KU
Earth Terminal Receive Frequency Range (GHz)	13.75-14.6
Latitude of Location	10.95-12.75
Longitude of Location	Block Converter
Downconverter Tuning Resolution	750 MHz
Downconverter Bandwidth	Block Converter
Automatic Power Control Capability	>250MHz
Automatic Power Control Level	No
Auto Tracking (Yes/No)	Not Applicable
Nominal Gain-to-Noise-Temperature	Yes
Saturated	2dBi/K
Linear Effective Isotropic Radiated Power	65.5dBW
Legend dBi/K    decibels relative to isotopic in kilowatts dBW    decibel watt GHz    gigahertz MHz    megahertz MVO    magnitude versus offset	

This page intentionally left blank.

# Glossary

The glossary lists acronyms and terms with Army or joint definitions. Where Army and joint definitions differ, (Army) precedes the definition. ATP 6-02.12 is not the proponent for any Army terms. The proponent publication for terms is listed in parentheses after the definition.

## SECTION I – ACRONYMS AND ABBREVIATIONS

<b>ACAS</b>	Army Centralized Army Request System
<b>ACES</b>	Automated Communications Engineering Software
<b>ADP</b>	Army doctrine publication
<b>AR</b>	Army regulation
<b>ATP</b>	Army techniques publication
<b>COMSEC</b>	communications security
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DOD</b>	Department of Defense
<b>DODI</b>	Department of Defense instruction
<b>DODIN</b>	Department of Defense information network
<b>DODIN-A</b>	Department of Defense information network-Army
<b>EW</b>	electromagnetic warfare
<b>G-2</b>	assistant chief of staff, intelligence
<b>G-3</b>	assistant chief of staff, operations
<b>G-6</b>	assistant chief of staff, signal
<b>HF</b>	high frequency
<b>IP</b>	Internet protocol
<b>METT-TC</b>	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
<b>NIPRNET</b>	Non-classified Internet Protocol Router Network
<b>PACE</b>	primary, alternate, contingency, and emergency
<b>PMESII-PT</b>	political, military, economic, social, information, infrastructure, physical environment, and time
<b>S-2</b>	battalion or brigade intelligence staff officer
<b>S-3</b>	battalion or brigade operations staff officer
<b>S-6</b>	battalion or brigade signal staff officer
<b>SINCGARS</b>	single-channel ground and airborne radio system
<b>SIPRNET</b>	SECRET Internet Protocol Router Network
<b>SMART-T</b>	Secure Mobile Anti-Jam Reliable Tactical Terminal
<b>VHF</b>	very high frequency
<b>WIN-T</b>	Warfighter Information Network-Tactical

## 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)

### **area of operations**

An operational area defined by the joint force commander for land and maritime forces that should be large enough to accomplish their missions and protect their forces. (JP 3-0)

### **assumption**

A specific supposition of the operational environment that is assumed to be true, in the absence of positive proof, essential for the continuation of planning. (JP 5-0)

### **communications security**

The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called **COMSEC**. (JP 6-0)

### **cross domain solution**

A cross domain solution is a form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains. (CNSSI 4009)

### **cybersecurity**

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (DODI 8500.01)

### **cyberspace**

A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12)

### **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 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)

### **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**. See also **electromagnetic warfare**. (JP 3-85)

### **enemy**

A party identified as hostile against which the use of force is authorized. (ADP 3-0)

**frequency deconfliction**

A systematic management procedure to coordinate the use of the electromagnetic spectrum for operations, communications, and intelligence functions. See also electromagnetic spectrum management; electromagnetic warfare. (JP 3-85)

**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)

**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)

**line of sight**

The unobstructed path from a Soldier's weapon, weapon sight, electronic sending and receiving antennas, or piece of reconnaissance equipment from one point to another. (ATP 2-01.3)

**military decision-making process**

An iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order. (ADP 5-0)

**network transport**

The processes, equipment, and transmission media that provide connectivity and move data between networking devices and facilities. (FM 6-02)

**operational environment**

A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. Also called OE. (JP 3-0)

**planning**

The art and science of understanding a situation, envisioning a desired future, and determining effective ways to bring that future about. (ADP 5-0)

**running estimate**

The continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if planned future operations are supportable. (ADP 5-0)

**spectrum management operations**

The interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations. (FM 6-0)

**synchronization**

1. The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. 2. In the intelligence context, application of intelligence sources and methods in concert with the operation plan to answer intelligence requirements in time to influence the decisions they support. (JP 2-0)

**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)

This page intentionally left blank.



# References

All URLs accessed on 6 July 2021.

## REQUIRED PUBLICATIONS

These documents must be available to intended users of this publication.

*DOD Dictionary of Military and Associated Terms*. August 2021.

FM 1-02.1. *Operational Terms*. 9 March 2021.

FM 1-02.2. *Military Symbols*. 11 November 2020.

## RELATED PUBLICATIONS

These documents contain relevant supplemental information.

## CHAIRMAN OF THE JOINT CHIEFS OF STAFF PUBLICATIONS

Most Chairman of the Joint Chiefs of Staff Publications are available at:

<https://www.jcs.mil/Library/CJCS-Instructions/>

CJCSI 5128.01. *Mission Partner Environment Executive Steering Committee (MPE ESC) Governance and Management*. 1 October 2014.

CJCSI 6250.01F. *Department of Defense Satellite Communications*. 26 February 2019.

## DEPARTMENT OF DEFENSE PUBLICATIONS

Most Department of Defense Instructions are available online:

<https://www.esd.whs.mil/DD/DoD-Issuances/>.

DODI 8110.01. *Mission Partner Environment Information Sharing Capability Implementation for the DOD*. 30 June 2021.

DODI 8500.01. *Cybersecurity*. 14 March 2014, Incorporating Change 1, 17 October 2019.

## JOINT PUBLICATIONS

Most joint publications are available online: <https://www.jcs.mil/doctrine>.

JP 2-0. *Joint Intelligence*. 22 October 2013.

JP 3-0. *Joint Operations*. 17 January 2017, Incorporating Change 1, 22 October 2018.

JP 5-0. *Joint Planning*, 1 December 2020.

JP 3-12. *Cyberspace Operations*. 8 June 2018.

JP 3-85. *Joint Electromagnetic Spectrum Operations*. 22 May 2020.

JP 6-0. *Joint Communications System*. 10 June 2015, Incorporating Change 1, 04 October 2019.

## ARMY PUBLICATIONS

Most Army doctrinal publications are available online: <https://armypubs.army.mil>.

ADP 3-0. *Operations*. 31 July 2019.

ADP 3-90. *Offense and Defense*. 31 July 2019.

ADP 5-0. *The Operations Process*. 31 July 2019.

ADP 6-22. *Army Leadership and the Profession*. 31 July 2019.

AR 380-10. *Foreign Disclosure and Contacts with Foreign Representatives*. 14 July 2015.

AR 381-12. *Threat Awareness and Reporting Program*. 1 June 2016.

ATP 1-02.1/MCRP 3-30B.1/NTTP 6-02.1/AFTTP 3-2.5. *Multi-Service Tactics, Techniques, and Procedures for Multi-Service Brevity Codes*. 28 May 2020.

ATP 2-01.3. *Intelligence Preparation of the Battlefield*. 1 March 2019.

ATP 3-12.3. *Electronic Warfare Techniques*. 16 July 2019.

ATP 4-33. *Maintenance Operations*. 9 July 2019.

ATP 6-0.5. *Command Post Organization and Operations*. 1 March 2017.

ATP 6-02.53. *Techniques for Tactical Radio Operations*. 13 February 2020.

ATP 6-02.54. *Techniques for Satellite Communications*. 05 November 2020.

ATP 6-02.60. *Tactical Networking Techniques for Corps and Below*. 9 August 2019.

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.

FM 3-0. *Operations*. 6 October 2017.

FM 3-09. *Fire Support and Field Artillery Operations*. 4 April 2014.

FM 6-0. *Commander and Staff Organization and Operations*. 5 May 2014.

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.

GTA 11-02-001. *Retrans Mission Checklist*. 11 April 2019.

TC 6-02.1. *The United States Army Signal Corps 2019 Training Strategy*. 11 July 2019.

TC 6-02.21. *Secure Mobile Anti-Jam Reliable Tactical-Terminal (SMART-T) Handbook*. 3 July 2019.

TC 7-100. *Hybrid Threat*. 26 November 2010.

## OTHER PUBLICATIONS

American, British, Canadian, Australian, New Zealand Armies Program Standards Number 2100 Edition 4, and Coalition Wide-Area Network, Network Operations, and Planning can be found at <https://wss.apan.org/cda/abcanz-armies>. (Registration is required.)

ABCANZ Standard Number 2105(R) Edition 4. *Network Operations Joining, Maintaining and Exiting Instructions*. <https://wss.apan.org/cda/abcanz-armies>. (Registration is required.)

Committee on National Security Systems Publications are available at: <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>. CAC Required.

CNSSI 4005. (U) *Safeguarding Communications Security (COMSEC) Facilities and Materials*. 22 August 2011.

CNSSI 4009. *Committee on National Security Systems (CNSS) Glossary*. 6 April 2015.

National Institute of Standards and Technology, Special Publication 800-207. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>

## RECOMMENDED READINGS

ADP 1-01. *Doctrine Primer*. 31 July 2019.

AR 25-1. *Army Information Technology*. 15 July 2019.

AR 25-2. *Army Cybersecurity*. 4 April 2019.

FM 3-94. *Armies, Corps, and Division Operations*. 23 July 2021.

FM 3-96. *Brigade Combat Team*. 19 January 2021.

## **WEBSITES**

Army Centralized Army Service Request System Website and Regional Hub Node Playbooks can be found here: <https://acas.army.mil/>. (Requires DOD-approved certificate login and user account.)

*Cyber Lessons and Best Practices Website:* <https://lwn.army.mil/web/cbl/home>. (Requires DOD-approved certificate login.)

## **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/>.

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

This page intentionally left blank.

# Index

Entries are by paragraph number.

**A**  
annex H (Signal), 2-22

**C**  
combat net radio, 3-36  
command post  
  setup, 4-20  
Command Post Node, B-4  
commercial satellite  
  communications, 3-19  
communications security  
  callout message, A-35  
coordination with staff  
  elements, 1-38  
cryptographic networks  
  planning, 3-107  
cybersecurity, 3-63  
  security domain, 3-65  
cybersecurity incident battle  
  drill, A-7  
cybersecurity incident report,  
  A-8

**D**  
defining signal requirements, 2-  
  12  
Defense Information Systems  
  Agency, 1-53, 3-26  
device hardening, 3-85  
digital fires, A-27

**E**  
electromagnetic spectrum, 1-7

**F**  
firewall, 3-77  
frequency assignment, 3-97

**G**  
global agile integrated  
  transport, 3-10  
guarded frequencies, A-32

**H**  
high frequency radios, 3-49

highband networking radio, 3-  
  33  
host-nation coordination, 3-105

**I**  
information dissemination  
  management and content  
  staging, 3-81  
congested environment, 1-8  
  contested environment, 1-  
  11  
information services, 3-1, 3-9  
internet protocol, 3-66

**J**  
Joint Integrated Satellite  
  Communications Tool, 3-17  
Joint Network Node, B-1  
joint restricted frequency list, A-  
  32  
joint spectrum interference  
  resolution report, A-33  
Joint-Tactical Network  
  Operations Toolkit, 3-104

**K**  
Key Management  
  Infrastructure, 3-27  
known supersession dates, A-  
  36

**L**  
line-of-sight, 3-30  
  high throughput, 3-31  
  terrestrial, 3-32  
link establishment, 4-23  
link-16, 3-53  
logistics staff, 1-46  
lower tier tactical internet, 1-58

**M**  
maintenance, 1-48  
military decision-making  
  process, 1-31  
mission partner environment,  
  1-60

mission variables, 1-33

**N**  
narrowband, 3-29  
network, 1-52  
  army, 1-55  
  joint, 1-52  
network engineer, 3-21  
network hardening, 3-82  
network monitoring, A-11  
network outage, A-10  
  report, A-10  
network transport, 3-1

**O**  
operational environment, 1-1—  
  1-2  
operational environment  
  considerations, 1-36  
operational variables, 1-33  
  economic, 1-33  
  infrastructure, 1-33  
  military, 1-33  
  physical environment, 1-33  
  political, 1-33  
  social, 1-33  
  time, 1-33  
operations staff, 1-39

**P**  
Phoenix Terminal, B-9  
planning, 1-28  
planning processes, 1-28  
point of presence, B-6  
primary, alternate, contingency,  
  and emergency  
  communications plan, 2-15  
priorities of work, 4-19  
protected frequencies, A-32  
protected satellite  
  communications, 3-20

## Entries are by paragraph number

**Q**

quality of service, 3-79

**R**

radio loadsets, 3-100

rapid decision making and  
synchronization process, 1-33

rapid decision-making, 1-34

reconnaissance, 4-17

Reduced Attack Surface, 3-87

regional hub node, 3-59

Regional Satellite  
Communications Support  
Center, 3-24

Retransmission, 3-40  
planning, 3-43

retransmission, A-5, A-23

**S**

satellite, 3-3

frequency division multiple  
access, 3-8

time division multiple  
access, 3-9

wideband, 3-7

satellite access request  
army centralized army  
service request, 3-15

gateway access request, 3-  
14

satellite communications  
transport, 3-3

satellite transportable terminal,  
B-8

signal operating instructions, 3-  
98

signal staff estimate, 2-1  
assumptions, 2-6  
civil considerations, 2-10  
conclusions and  
recommendations, 2-11  
enemy activities and  
capabilities, 2-9  
facts, 2-5  
friendly force status, 2-8

signature reduction, 4-28  
visual, 4-29  
electromagnetic, 4-34  
infrared, 4-43  
light discipline, 4-32  
noise, 4-41  
radar, 4-42

site planning, 4-11

site reconnaissance, 4-17

site security and defense, 4-24

site selection, 4-1  
antenna placement, 4-8  
link geometry, 4-5

signal site analysis, 4-2  
terrain masking, 4-7

site selection, 4-1

spectrum manager, 3-23

spectrum planning  
frequency deconfliction, 3-  
94

spectrum planning, 3-89

strong authentication, 3-84

supply, 1-47

**T**

taboo frequencies, A-32

tactical communications node,  
B-5

tactical flexible multiplexer, B-3

threats, 1-15

hybrid threat, 1-20

information warfare, 1-22

insider threat, 1-25

peer, 1-17

time division multiple access  
network centric waveform,  
3-9

troop leading procedures, 1-35

tropospheric scatter, 3-35

**U**

upper tier tactical internet, 1-57

**ATP 6-02.12**

**17 November 2021**

By Order of the Secretary of the Army:

**JAMES C. MCCONVILLE**

*General, United States Army  
Chief of Staff*

Official:

A handwritten signature in black ink, appearing to read 'Mark F. Averill', written in a cursive style.

**MARK F. AVERILL**

*Acting Administrative Assistant  
to the Secretary of the Army*

2130700

**DISTRIBUTION:**

*Active Army, Army National Guard, and United States Army Reserve. Distributed in  
electronic media only(EMO).*

