ATP 6-02.60

TACTICAL NETWORKING TECHNIQUES FOR CORPS AND BELOW

AUGUST 2019

This publication supersedes ATP 6-02.60, dated 3 February 2016.

Headquarters, Department of the Army

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

*ATP 6-02.60

Army Techniques Publication
No. 6-02.60

Headquarters
Department of the Army
Washington, D.C., 9 August 2019

Tactical Networking Techniques for Corps and Below

Contents

* This publication supersedes ATP 6-02.60, dated 3 February 2016

Figures

Tables

Preface

ATP 6-02.60 builds on the tactical communications information provided in FM 6-02. This manual establishes non-prescriptive ways to perform missions, functions, and tasks to provide the upper tier tactical internet that enables command and control in support of large-scale combat operations.

The principal audience for ATP 6-02.60 is Army Professionals who plan, install, operate, maintain, and secure the tactical network. Commanders and staffs of Army headquarters serving as joint task force or multinational headquarters should also refer to applicable joint or multinational doctrine concerning the range of military operations and joint or multinational forces. Trainers and educators throughout the Army will also use this publication.

Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable U.S., international, and, in some cases, host-nation laws and regulations. Commanders at all levels ensure their Soldiers operate in accordance with the law of war and the rules of engagement (see FM 6-27). They also adhere to the Army Ethic as described in ADP 1.

ATP 6-02.60 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. Terms for which ATP 6-02.60 is the proponent publication (the authority) are marked with an asterisk (*) in the glossary. Definitions for which ATP 6-02.60 is the proponent publication are boldfaced in the text. For other definitions shown in the text, the term is italicized, and the number of the proponent publication follows the definition.

This publication applies to the Active Army, Army National Guard/Army National Guard of the United States, and United States Army Reserve unless otherwise stated.

The proponent 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-OP (ATP 6-02.60), 506 Chamberlain Avenue, Fort Gordon, GA 30905-5735, or via e-mail to usarmy.gordon.cyber-coe.mbx.gord-fg-doctrine@mail.mil.

This page intentionally left blank.

Introduction

ATP 6-02.60 outlines doctrinal techniques for implementing the tactical network at echelons corps and below in support of unified land operations. The tactical network provides deployed warfighters reliable, mobile communications and connects them to the Department of Defense information network-Army.

To apply the techniques contained in this publication, readers should be familiar with ADP 1, ADP 3-0, and FM 3-0 to understand how Army forces conduct operations as part of joint force in large-scale combat operations. Commanders and network planners should also be familiar with FM 6-02 and ATP 6-02.71 to understand the role of signal formations and staffs in support of Army operations.

ATP 6-02.60 supersedes ATP 6-02.60, dated 3 February 2016. The changes incorporate updated concepts, terminology, and Department of Defense information network operations techniques.

This publication contains four chapters and two appendixes—

Chapter 1 provides an overview of the tactical network. It begins with the discussion of the contested and congested operational environment, then discusses the joint global and theater network (the Department of Defense information network) and the Department of Defense information network-Army.

Chapter 2 discusses tactical networking systems and equipment. Section I provides a brief description of Warfighter Information Network-Tactical and its means of network transport. It goes on to introduce colorless core routing and tunneling of top secret sensitive compartmented information networks through the Warfighter Information Network-Tactical wide-area network. Section II discusses the equipment that make up the Warfighter Information Network-Tactical and the communications capabilities of the various node types.

Chapter 3 discusses management of the tactical network, including Department of Defense information network operations, cybersecurity, the network operations and security center, network management functions and software, network planning, network and node management, quality of service and speed of service management, configuration management, and prioritizing information to align with the commander's intent.

Chapter 4 discusses employment of Warfighter Information Network-Tactical by echelon. Section I discusses support to the various command post types and command post survivability. Section II discusses employment of Warfighter Information Network-Tactical at echelons corps through battalion, multifunctional support brigade, and expeditionary signal battalion. Section III discusses individual and crew training, and unit collective training for tactical signal systems.

Appendix A discusses tactical signal support in a contested environment. It discusses peer threat tactics, techniques, and procedures and introduces techniques to prevent, recognize, and respond to threat effects in cyberspace and the electromagnetic spectrum.

Appendix B discusses maintenance. It discusses maintenance management, the two-level maintenance system, and communications-electronics maintenance at the division and below.

This page intentionally left blank.

Chapter 1

Introduction to the Tactical Network

This chapter introduces the tactical network at corps and below. Section I gives an overview of the expected operational environment when conducting large-scale combat operations against a peer threat. Section II introduces the joint global and theater network, the Department of Defense information network-Army, and the upper tier and lower tier tactical internet.

SECTION I – THE INFORMATION ENVIRONMENT

1-1. U.S. forces seek to dominate the information environment to maintain information advantage. The *information environment* is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information (JP 3-13). Cyberspace and the electromagnetic spectrum are parts of the information environment. The information environment, in turn, is part of the overall operational environment. Effects in the information environment may affect other decisions and conditions in the operational environment.

CONGESTED ENVIRONMENT

1-2. Competition for the limited available bandwidth results in a congested electromagnetic spectrum, particularly when operating in developed nations. Within the electromagnetic spectrum, joint forces contend with civil agencies, commercial entities, allied forces, and adversaries for use of a common electromagnetic spectrum resource (ATP 6-02.70). Gaining and maintaining control of the electromagnetic spectrum is a critical requirement for the commander. From communications, to intelligence collection, to electronic warfare, all forces and supporting agencies depend on the electromagnetic spectrum to execute operations in the air, land, maritime, space, and cyberspace domains.

CONTESTED ENVIRONMENT

1-3. Enemies and adversaries may deliberately attempt to deny friendly use of the electromagnetic spectrum, space, cyberspace, and/or terrestrial systems. Due to heavy reliance on advanced communications systems, such an attack may be a central element of any enemy or adversary anti-access and area denial strategy, requiring a higher degree of protection for friendly command and control systems and planning for operations in a denied or degraded environment (JP 6-0).

1-4. U.S. forces dominated cyberspace and the electromagnetic spectrum in Afghanistan and Iraq against adversaries who lacked the technical capabilities to compel the coalition to contend with a contested environment. More recently, regional peers have demonstrated impressive capabilities in a hybrid operational environment. These adversary capabilities threaten U.S. freedom of action in cyberspace and the electromagnetic spectrum.

1-5. U.S. military communications and information networks are key command and control enablers. For this reason, they present high-value targets for enemies and adversaries. Technologically sophisticated adversaries understand the extent of U.S. forces' reliance on communications and automated information systems. In future conflicts, U.S. forces should expect enemies and adversaries to contest the information environment to deny operational access and diminish the effectiveness of U.S. and allied forces.

1-6. Degraded capabilities may result from threat actions, but may also occur due to insufficient resources in the operational area. They may also result from a lack of coverage—such as inadequate communications

satellite capacity—in the operational area, or from electromagnetic interference, whether intentional (jamming) or unintentional.

1-7. Successfully integrating signal support with cyberspace, electronic warfare, and intelligence capabilities is the key to obtaining and maintaining freedom of action in cyberspace and the electromagnetic spectrum, and the ability to deny the same to our adversaries. Synchronizing capabilities across multiple domains and warfighting functions maximizes their inherently complementary effects in and through cyberspace and the electromagnetic spectrum (ATP 6-02.71).

1-8. U.S. military networks face continuous cyberspace risk from a variety of threat sources. Every day DOD networks come under attack by threat agents, including—

- Unauthorized users.
- Insiders.
- Terrorist groups.
- Non-state actors (criminal and activist organizations).
- Foreign intelligence entities.
- Military or political opponents.

1-9. The persistent nature of the cyberspace risk causes U.S. forces to expend a great deal of resources and effort securing and defending DOD networks. Network-enabled operations are a force multiplier and a traditional strength of U.S. forces, but network-enabled operations also create significant vulnerabilities. The extent to which U.S. forces rely on networks and networked capabilities presents broad cyberspace and electronic warfare attack surfaces. Each network device and capability becomes a potential attack vector an adversary may seek to exploit. Failing to protect even one system can give an adversary a foothold into the Department of Defense information network (DODIN) and place sensitive data, U.S. operations, and lives at risk. Even when cyberspace defenders discover and stop an attack, it is not always possible to attribute the attack to a particular source. Following cybersecurity best practices, maintaining active cyberspace defense, and adhering to operations security guidelines help protect DOD networks and data. Refer to FM 6-02 for more detailed discussion of threat effects on signal support in a contested environment.

SECTION II – NETWORK OVERVIEW

JOINT NETWORK

1-10. The *Department of Defense information network* is the set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems (JP 6-0).

1-11. As the DOD portion of cyberspace, the DODIN interacts with and provides connections to national and global cyberspace. The DODIN encompasses the Service-specific enclaves of the Army, Navy, Air Force, and Marine Corps combined with joint capabilities provided by the Defense Information Systems Agency. An *enclave* is a collection of computing environments connected by one or more internal networks under the control of a single authority and security policy (CNSSI 4009).

DEFENSE INFORMATION SYSTEMS NETWORK

1-12. The Defense Information Systems Network (DISN) is the joint portion of the DODIN operated by the Defense Information Systems Agency. DISN services include SECRET Internet Protocol Router Network (SIPRNET), Non-classified Internet Protocol Router Network (NIPRNET), and video teleconferencing.

THEATER NETWORK

1-13. The theater network consists of the systems and devices controlled by the geographic combatant command and its Service components. The theater network provides in-theater access to DISN and theater-specific information services. Geographic combatant commanders direct DODIN operations within their

respective areas of responsibility. *Department of Defense information network operations* are operations to secure, configure, operate, extend, maintain, and sustain Department of Defense cyberspace to create and preserve the confidentiality, availability, and integrity of the Department of Defense information network (JP 3-12).

1-14. Signal leaders and staffs plan communications and network capabilities to support all anticipated requirements in their operational area. However, in a degraded or denied environment, there may not be enough communications capacity to support all missions. Changes in the operational variables (political, military, economic, social, information, infrastructure, physical environment, and time) or mission variables (mission, enemy, terrain and weather, troops and support available, time available, and civil considerations) may change communications requirements beyond the capabilities of assigned and attached signal elements. Theater DODIN operations responsibilities align to the operational chain of command for unity of command and unity of effort. This alignment allows commanders to allocate available communications and network support to their highest mission priorities until additional capabilities are available.

GLOBAL AGILE INTEGRATED TRANSPORT

1-15. DOD gateways connect with one another through the Defense Information Systems Agency's global agile integrated transport. The global agile integrated transport architecture uses a high-speed fiber optic backbone to transport data between gateway sites, or from the home station to a DOD gateway site for relay to deployed elements. Global agile integrated transport reduces the need for multi-hop satellite communications paths. Global agile integrated transport eliminates the need to transfer data from a regional hub node over a satellite back to home station or another global location. Global agile integrated transport architecture simplifies the network and supports planning, DODIN operations, and troubleshooting.

ARMY NETWORK

1-16. The *Department of Defense information network-Army* (DODIN-A) 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.

STRATEGIC INFRASTRUCTURE

1-17. The strategic network provides fixed infrastructure that supports operations in garrison and provides access points to connect deployed tactical forces to the DODIN-A. The strategic network provides expeditionary forces reachback and access to DISN services, regardless of where their mission takes them. *Reachback* is the process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed (JP 3-30).

1-18. Because the network architecture and cybersecurity configurations are common across theaters, expeditionary units can enter a theater with their automated information systems preconfigured, ready to connect with the theater infrastructure and quickly establish communications and DISN services. Refer to ATP 6-02.71 for more information about the strategic portion of the DODIN-A.

TACTICAL INTERNET

1-19. 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

1-20. 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. 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) provides 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. This publication deals primarily with operation of the upper tier tactical internet.

Lower Tier

1-21. The lower tier tactical internet supports tactical formations down to the team leader. The lower tier consists primarily of single-channel radio networks at platoons and companies. The primary lower tier waveforms are Soldier radio waveform and the single-channel ground and airborne radio system. Mobile applications enable visualization, operator interface with ancillary devices (such as Global Positioning System), targeting data, voice communications, and sensor capability. Refer to ATP 6-02.53 for more information about the lower tier tactical internet.

Chapter 2

Warfighter Information Network-Tactical

Warfighter Information Network-Tactical is an integrated communications system of systems that provides network transport and information services and the secret and unclassified local area networks. Networking, transport, and Department of Defense information network operations components are interoperable across all system configurations.

SECTION I – WARFIGHTER INFORMATION NETWORK-TACTICAL OVERVIEW

OVERVIEW

2-1. WIN-T integrates networking hardware and software with line of sight and satellite communications transport. WIN-T systems connect deployed units to the DODIN-A to provide secure mobile communications, support situational understanding, and enable command and control while supporting the other warfighting functions. Organic WIN-T capabilities at echelons corps through battalion provide a secure, distributed network with robust network services in support of unified land operations.

2-2. The configuration and equipment complement of WIN-T is dependent on echelon and unit type. Active duty divisions and brigade combat teams use WIN-T increment 2 systems to extend services both at-the-halt and on-the move. Corps, Reserve Component divisions, multifunctional support brigades, and expeditionary signal battalions use increment 1b systems to extend services to deployed units at-the-halt.

INCREMENT 1B

2-3. WIN-T Increment 1b provides high-throughput voice, data, and video communications to support command posts down to battalion level at-the-halt. WIN-T increment 1b-equipped units include the corps, Reserve Component divisions, multifunctional support brigades, and expeditionary signal battalions.

INCREMENT 2

2-4. Active Component divisions and brigade combat teams are equipped with WIN-T increment 2. Increment 2 systems provide the same information services as increment 1b with the following additional capabilities—

- Networking line of sight radios to establish a self-forming and self-healing network.
- DODIN operations, network planning, and network monitoring capabilities integrated into the network architecture.
- Ability to operate on-the-move as well as at-the halt.

NETWORK TRANSPORT

2-5. WIN-T systems combine line of sight and satellite communications network transport to enhance network reliability and to make best use of the advantages of each. The network prioritizes line of sight transport to minimize the demand for satellite transmission.

2-6. Satellite communications transport establishes initial network connectivity and reachback to the strategic portion of the DODIN-A to access DISN services. It also serves as a backup to line of sight transport for uninterrupted connection to critical services.

LINE OF SIGHT TRANSPORT

2-7. 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. The maximum range of a line of sight radio is approximately 40 kilometers, or 25 miles.

2-8. WIN-T line of sight radios are the high capacity line of sight radio and the Highband Networking Radio. Both increment 1b and increment 2 can use the high capacity line of sight. Only increment 2 uses the Highband Networking Radio.

SATELLITE COMMUNICATIONS TRANSPORT

2-9. Satellite communications provide significant advantages for an expeditionary force. Satellite communications transport provides—

- Global reach from the national command authority to deployed forces.
- Connection to DISN services in austere environments with no preexisting communications infrastructure.
- Immediate access to the DODIN on initialization.
- Access for isolated forces without terrain or distance limitations.
- Long-haul backbone data transport and reachback to the sustaining base.
- Communications that span beyond line of sight distances, terrain obstructions, or hostile forces.
- Communications on-the-move to mobile command vehicles, combat vehicles, and dismounted Soldiers.

2-10. Connecting the tactical network to the sustaining base via satellite communications transport provides full access to DISN services as soon as the first nodes establish the network. Despite its advantages, satellite communications also has drawbacks. Satellite bandwidth is costly and susceptible to transmission delays. Satellite bandwidth availability may be limited, particularly in some remote or sparsely populated regions. Satellite communications transport is also subject to degradation during severe weather.

Frequency Division Multiple Access

2-11. 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.

Time Division Multiple Access

2-12. With time division multiple access, many terminals share a given frequency and bandwidth block in time slots. Time division multiple access is a more efficient way to allocate limited satellite bandwidth, at the cost of relatively lower throughput as compared with frequency division multiple access. Battalion headquarters typically access the brigade and division network using time division multiple access. WIN-T increment 2 also uses time division multiple access for on-the-move networking.

2-13. Figure 2-1 on page 2-3, shows the key advantages satellite communications can provide. These advantages are common to satellite communications in general, not specific to WIN-T systems. For more information about satellite communications, refer to FM 3-14 and ATP 6-02.54.

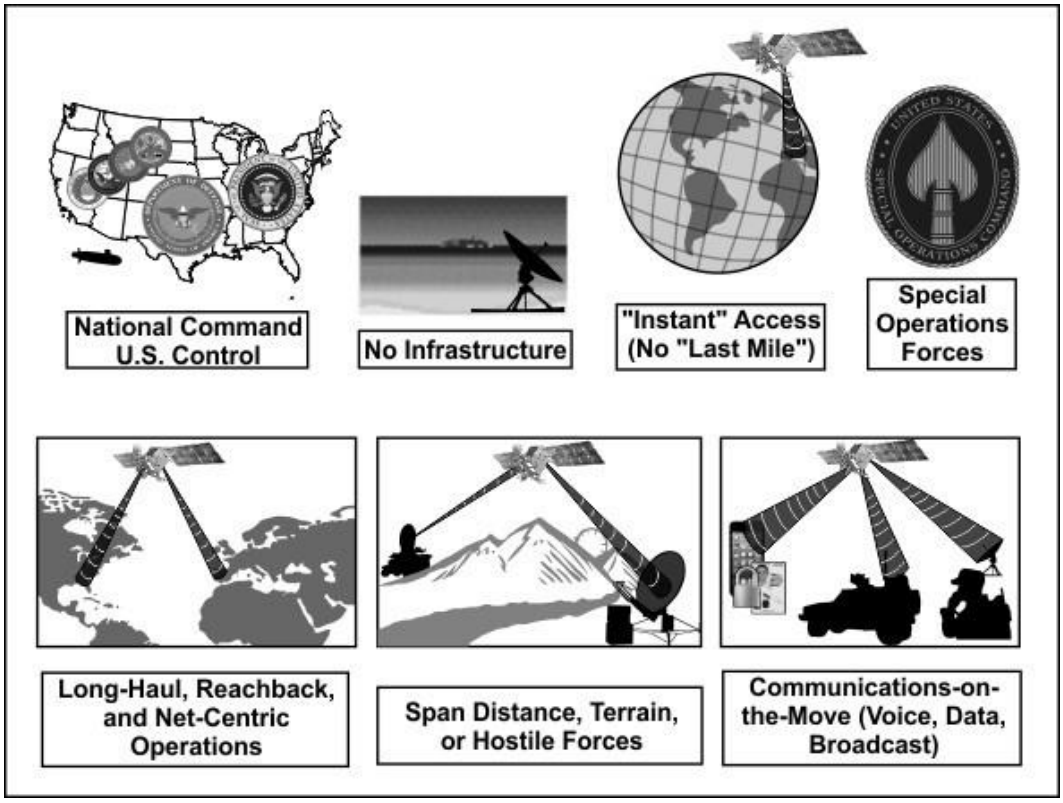

Figure 2-1. Key advantages of satellite communications

COLORLESS CORE

2-14. Colorless core is a Defense Information Systems Agency-compliant cybersecurity architecture that offers more efficient Internet protocol (IP) network encryption and transport. *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). The key benefits of colorless core are enhanced data protection and more efficient bandwidth use.

COMMUNICATIONS SECURITY AND TRANSMISSION SECURITY

2-15. With colorless core, both classified and unclassified data undergo encryption before passing over the network transport backbone (the wide-area network). Since all the encrypted data looks the same, an adversary cannot distinguish between classified and unclassified. This makes unclassified information just as hard to recover as classified information. It also makes it harder for adversaries to target classified networks for cryptanalysis.

2-16. In the colorless core architecture, data undergoes encryption twice—once at the network layer (communications security) and again at the link layer (transmission security). The data must also undergo decryption twice. Link layer encryption isolates the network backbone from external networks. User data decryption takes place after the data leaves the wide-area network at its destination.

2-17. Colorless core protects data in transit over the WIN-T wide-area network. TACLANEs provide transmission security encryption to isolate the network backbone. The TACLANE is a National Security Agency-approved type-1 communications security device.

2-18. On the SIPRNET and NIPRNET local area networks, routers and switches provide enclave protection, local area network extension, and local user access to DISN services. On the wide-area network, the TACLANE cryptographically isolates all user traffic from the wide-area network while the colorless routers provide a meshed transport network between WIN-T nodes.

2-19. The colorless core routing design consists of—

- SIPRNET and NIPRNET local area network routers hosting multiple IP subnets. The local area network router connects to a TACLANE for transmission security.
- TACLANEs encrypt data for tunneling through the wide-area network. The TACLANE uplink interface connects to the wide-area network router.
- The cluster of wide-area network routers forms the (colorless) core of the WIN-T network.

2-20. The SIPRNET and NIPRNET local area network data use separate user data encryption (communications security) at the local area network side of the wide-area network router before passing through the TACLANE for link encryption (transmission security). Only the encrypted colorless core data passes through the wide-area network.

TRANSPORT CONVERGENCE

2-21. The Joint Worldwide Intelligence Communications System and National Security Agency Network are military intelligence operated networks that provide division and brigade commanders and their intelligence elements access to top secret and sensitive compartmented information. The WIN-T colorless core tunnels sensitive compartmented information from the TROJAN Network Control Center through the regional hub node to deployed users. The data tunnel allows end users to send information back using the same path.

2-22. A type-1 encryption device cryptographically isolates sensitive compartmented information from SIPRNET and NIPRNET. WIN-T provides only network transport bandwidth for these networks. The assistant chief of staff, signal (G-6), battalion or brigade signal staff officer (S-6), and the division or brigade network operations and security center (NOSC) do not perform DODIN operations for sensitive compartmented information networks.

2-23. The assistant chief of staff, intelligence (G-2) and the battalion or brigade intelligence staff officer (S-2) at the division and brigade perform network engineering, accreditation, and DODIN operations for top secret and sensitive compartmented information networks, with policy guidance from the Deputy Chief of Staff, Intelligence. G-6 (S-6) staffs perform network engineering, accreditation, and DODIN operations for the wide-area network, with policy guidance from the Chief Information Officer/G-6

TROJAN Network Control Center

2-24. The TROJAN Network Control Center provides DODIN operations and information services for top secret and sensitive compartmented information networks. The TROJAN Network Control Center extends encrypted top secret and sensitive compartmented information data to the regional hub node for transmission over the WIN-T colorless core.

Regional Hub Node

2-25. The regional hub nodes provide network transport to extend top secret and sensitive compartmented information networks to deployed brigade and above units. The regional hub nodes only provide bandwidth; they do not process top secret data and have no DODIN operations responsibility for it. Figure 2-2 on page 2-5, depicts the colorless core with sensitive compartmented information networks tunneled through the wide-area network to access points at division and brigade.

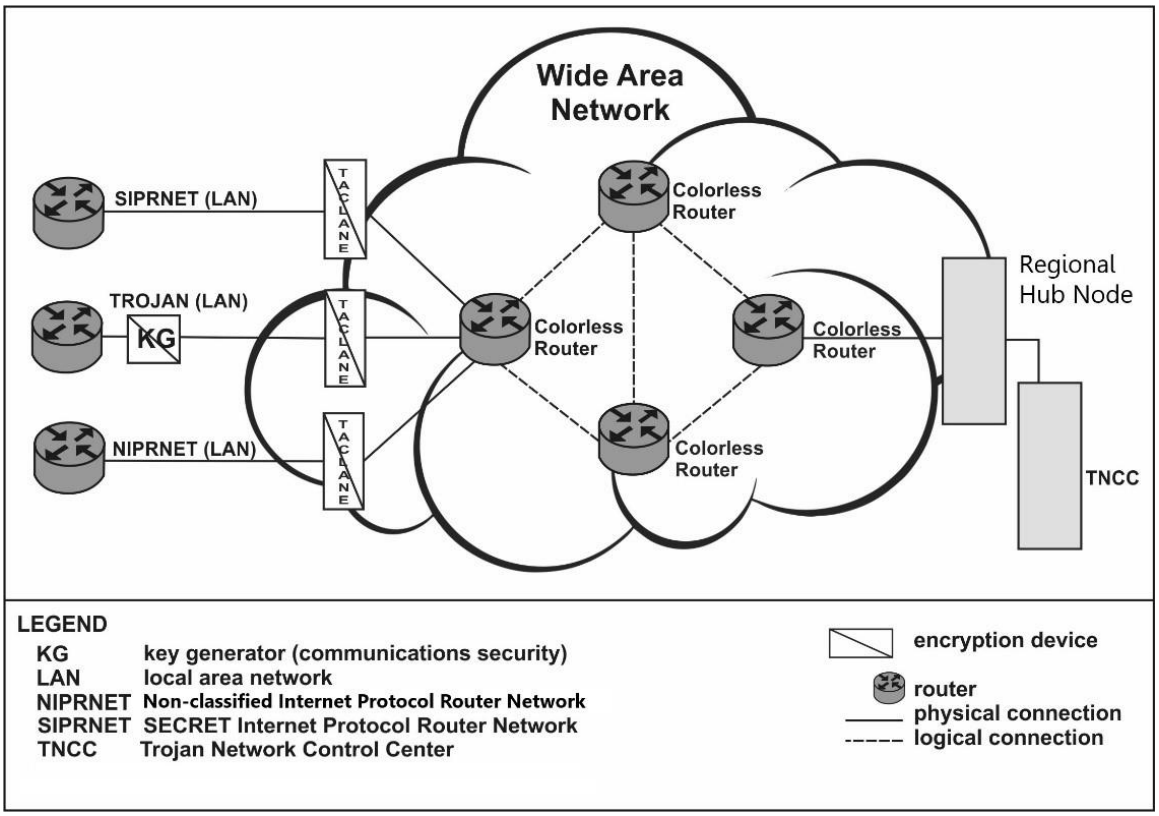

Figure 2-2. Colorless core with sensitive compartmented information tunneling

SECTION II – SYSTEM DESCRIPTION AND EQUIPMENT

EQUIPMENT COMMON TO INCREMENT 2 AND INCREMENT 1B

REGIONAL HUB NODE

2-26. The ***regional hub node*** **is the gateway transport node for the Warfighter Information Network-Tactical, and the transport medium for theater-based network service centers.** The regional hub node provides reachback and DISN services for increment 1b and increment 2-equipped units. The regional hub node also serves as a bridge to provide communications interoperability between units operating different equipment. The regional hub node provides the primary communications connection between deployed forces and the sustaining base. The regional hub node's satellite communications transport extends DISN services to deployed units. Major WIN-T nodes can connect to the regional hub node using either commercial Ku band or military Ka band satellites. United States Army Network Enterprise Technology Command pre-provisions commercial satellite bandwidth for the regional hub node to support contingencies.

2-27. The regional hub node is colocated with a DOD gateway site. Regional hub nodes operate in sanctuary (outside the combat zone) for access to DISN services. Regional hub nodes' strategic positioning provides global coverage to allow immediate access to secure and nonsecure data and voice communications. This allows units to accomplish their missions in any location. These missions may be close to the home station or in remote, austere environments where communications infrastructure often does not exist. Regional hub node access allows forces to mobilize without having to develop their own network access solutions.

2-28. Because the regional hub node operates full-time, deploying units can establish reachback communications much quicker. A unit may be able to establish initial communications and reachback capabilities within minutes, rather than requiring hours or days as with legacy systems.

2-29. The regional hub node permanently connects to a tier 1 network. It extends access to SIPRNET, NIPRNET, secure Voice over Internet Protocol (VoIP), video teleconferencing, the Defense Switched Network, and mission partner environment. The regional hub node provides transport of sensitive compartmented information networks from the TROJAN Network Control Center to deployed divisions and brigades. The regional hub node also provides enclave boundary protection (tier 1 to tier 2; SIPRNET to NIPRNET). Network centric waveform modems and colorless core routers at the regional hub node support both increment 1b and increment 2 satellite communications links.

TACTICAL HUB NODE

2-30. The tactical hub node is the central element of the division network. It connects to a DOD gateway via frequency division multiple access satellite communications link for access to DISN services. It distributes DISN services to subordinate command posts via time division multiple access satellite communications. The tactical hub node can extend DISN services and command and control-enabling services from the division to subordinate brigade combat teams where regional hub node service is not available. The tactical hub node may also augment a regional hub node.

2-31. The tactical hub node supports the organic WIN-T systems of one division. It merges the time division multiple access and frequency division multiple access satellite network architectures. The tactical hub node provides end-to-end network transport to extend DISN services to the deployed tactical network.

2-32. The tactical hub node consists of three major subsystems—the baseband shelter and two time division multiple access and frequency division multiple access-capable satellite communications shelters. In order to extend DISN services, the tactical hub node normally deploys to a DOD gateway site. When not located at a DOD gateway site, the hub node connects to the DOD gateway through a super high frequency satellite communications link for access to DISN services.

2-33. Tactical hub node capabilities include—

- **SIPRNET and NIPRNET VoIP call control**. Includes call forwarding, call transfer, redial, and conference bridging.
- **DISN services**. SIPRNET and NIPRNET.
- **Video teleconferencing.** Classified and non-classified.
- **Private branch exchange service.** Analog telephone service.
- **Enclave boundary protection.** Tier 2 perimeter router.
- **Colorless core.** Cryptographically isolated SIPRNET, NIPRNET, and sensitive compartmented information networks.
- **Satellite communications transport.** Commercial Ku band and military Ka band frequency division multiple access, time division multiple access, and network centric waveform.
- **Ethernet switching**. SIPRNET and NIPRNET local area network switches provide power over Ethernet for IP phones.
- **Fiber optic interface.** A multi-channel, synchronous time division digital multiplexer and fiber optic modem with tactical fiber optic cable assembly connections for interface with alternate network transport systems.
- **Alternate transport.** Can interface with high capacity line of sight, Phoenix satellite communications terminal, or Secure Mobile Anti-Jam Reliable Tactical Terminal (SMART-T) for alternate network transport capabilities.
- **Redundant Power.** Provided by either on-board or towed generators or utility power.

SATELLITE TRANSPORTABLE TERMINAL

2-34. The Satellite Transportable Terminal is a trailer-mounted, 2.4-meter Ku and Ka band satellite communications terminal. It provides beyond line of sight network transport for the Tactical Communications Node (TCN), Joint Network Node, and Command Post Node. The Satellite Transportable Terminal operates at-the-halt only.

2-35. There are two versions of the Satellite Transportable Terminal. One uses both frequency division multiple access and time division multiple access modems. This version supports the TCN and increment 1b Joint Network Node shelter. The second version uses time division multiple access only, and supports the increment 1b Command Post Node. While the Satellite Transportable Terminal can operate using its onboard generator, units should operate using an external 10-kilowatt generator whenever possible.

2-36. Satellite Transportable Terminal capabilities include—

- Commercial Ku band or military Ka band transmission.
- Frequency division multiple access.
- Network centric waveform.
- Local node management.

HIGH CAPACITY LINE OF SIGHT

2-37. The high capacity line of site terminal provides high-throughput line of sight network transport for fixed command posts. The high capacity line of sight terminal provides much greater bandwidth and lower operating cost than the Satellite Transportable Terminal, but it is limited to line of sight ranges. The high capacity line of sight radio is capable of up to 16 megabits per second data throughput, depending on the radio band selected.

2-38. In increment 2, the high capacity line of sight terminal provides alternate network transport for the division and brigade TCNs to support the main, tactical, and support area command posts at-the-halt. The high capacity line of sight system interfaces with the TCN via the tactical fiber optic cable assembly.

2-39. In increment 1b, the high capacity line of sight terminal provides alternate network transport for the Joint Network Node and Command Post Node. The high capacity line of sight system interfaces with the Joint Network Node shelter via the tactical fiber optic cable assembly.

MODULAR COMMUNICATIONS NODE-ENHANCED ENCLAVE

2-40. The Modular Communications Node-Advanced Enclave provides access to sensitive compartmented information networks at echelons brigade and above. The Modular Communications Node-Advanced Enclave provides sensitive compartmented information user services and interfaces with the WIN-T colorless core for network transport. The Modular Communications Node-Advanced Enclave consists of two user access cases. Each user case serves one security enclave.

COMMERCIAL COALITION EQUIPMENT

2-41. Commercial coalition equipment provides access to commercial or coalition voice, video, and data services. Commercial coalition equipment provides radio bridging and voice cross-banding to enable radios on different frequencies to connect with other inter-organizational partners. The commercial coalition equipment supports static command posts. The commercial coalition equipment accesses the DODIN-A through either satellite communications or high capacity line of sight link to the Joint Network Node, or satellite communications to the hub node.

2-42. The system is contained in a small form factor case for commercial transport. The commercial coalition equipment provides two removable hard drives for immediate declassification and re-use in different security enclaves. The supported battalion or brigade S-6 controls network services from the command post.

INCREMENT 2

2-43. Increment 2 nodes enable command and control on-the-move as well as at-the-halt. WIN-T increment 2 line of sight and satellite communications transport systems provide redundant transmission paths for more reliable connectivity and self-healing networks. The network integrates division, brigade combat team, and battalion commanders so they can conduct operations while maintaining contact with higher, subordinate, and adjacent headquarters.

2-44. WIN-T increment 2 provides voice, video and data exchange from Army divisions to brigade combat teams, down to battalion level. The network architecture supports the fundamental principles of signal support:

- **Operational focus**—WIN-T systems allow division, brigade, and battalion leaders to access the DODIN-A in any environment. Commanders exercise command authority over their respective portions of the network to manage the network as a warfighting platform.
- **Interoperability**.
  - Compatibility—systems are compatible and interoperable at all echelons across the DODIN-A. This includes beyond line of sight communications capabilities and links to the upper tier and lower tier tactical internet.
  - Standardization—provides interoperability between legacy, current, and planned future networks, and with joint, inter-organizational, and multinational mission partners.
- **Agility**—provides network resources for each operational phase, and supports task reorganization to move resources between commands based on time, phase-lines, location, and mission variables.
  - Capacity—organic systems have the capability to support all network requirements in the main command post, tactical command post, and mobile command group.
  - Flexibility—modular systems can be re-tasked as necessary to satisfy contingency and emergent requirements.
  - Mobility—enables division, brigade combat team, and battalion command and staff at-the-halt and on-the-move. Command post systems can displace rapidly.
  - Redundancy—implements communications-in-depth using wired, line of sight, and satellite communications network transport.
  - Reliability—network management software manages bandwidth and transmission paths automatically to bypass outages and congestion. Systems have high on-line availability rates.
  - Scalability—allows commands to scale the network to any size operation from limited initial entry packages to theater-wide tactical networks supporting large-scale combat operations.
  - Timeliness—rapid network establishment using satellite communications for reachback and instant access to DISN services.
- **Trusted systems**.
  - Protection—cybersecurity defense-in-depth integrated into the network architecture.
  - Survivability—integrates robust cyber network defenses into the system to protect against an advanced cyber threat capabilities. The virtual firewall and improved software tools are effective against a range of threat tactics, techniques, and procedures.
  - Sustainability—organic maintenance support elements can maintain and repair systems with on-hand spares and return them to service quickly.
- **Shared networks**—common standards to operate with joint, inter-organizational, and multinational mission partners.
- **Network situational awareness**—NOSC maintains a comprehensive, map-based network situational awareness view.

TACTICAL COMMUNICATIONS NODE

2-45. The TCN is the core of the increment 2 network. It provides network services using line of sight and satellite communications transport, both on-the-move and at-the-halt. The TCN can interface with the high capacity line of sight terminal or Satellite Transportable Terminal for higher throughput network transport at-the-halt only. The following unit types have TCNs—

- Division headquarters.
- Brigade combat team headquarters.
- Maneuver battalion headquarters.

2-46. A TCN may operate with a Tactical Relay-Tower or a NOSC. A Satellite Transportable Terminal accompanies each TCN to provide higher-throughput satellite communications transport at-the-halt. A TCN

can also interface with a SMART-T or high capacity line of sight terminal for alternate network transport at-the-halt.

2-47. TCN capabilities include—

- **SIPRNET and NIPRNET VoIP call control.** Unified Communications Manager also acts as an IP private branch exchange to provide call forwarding, call transfer, redial, and conference bridging.
- **Combat net radio interface.** Connects combat net radios to a VoIP network.
  - Provides a half-duplex connection between the combat net radio and the WIN-T IP infrastructure.
  - Connects two different combat radio networks together through the WIN-T network.
  - Provides telephone signaling and conversion from analog to digital.
  - Extends combat net radio ranges beyond line of sight using WIN-T satellite communications transport.
- **Ethernet switching.** SIPRNET and NIPRNET local area network switches provide power over Ethernet for IP phones. Power over Ethernet eliminates the need for power adapters when connecting IP phones to the switches. Both the switch and the telephone equipment must be power over Ethernet capable.
- **Fiber optic interface.** A multi-channel, synchronous time division digital multiplexer and fiber optic modem with tactical fiber optic cable assembly connections for line of sight interface.
- **Global Positioning System interface.** Provides positioning data and system timing.
- **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.
  - Highband Radio Frequency Unit is a directive-beam, C band antenna that supports high rate data, both on-the-move and at-the-halt.
  - The Range Throughput Extension Kit is a fixed-beam, higher-gain antenna for operations at-the-halt only.
- **Inertial navigation.** Provides continuous, accurate vehicle position, velocity, and attitude reporting to improve the Highband Radio Frequency Unit antenna pointing accuracy. This allows on-the-move antennas to react to vehicle motion and maintain accurate pointing.
- **Network centric waveform.** Uses spread spectrum, multi-channel modulation and demodulation, advanced turbo coding, and advanced encryption standard encryption and decryption for satellite communications interface.
- **Routing—**
  - Colorless (wide-area network). Cryptographically isolated from the SIPRNET and NIPRNET local area network routers. It serves as cybersecurity perimeter protection. The colorless router includes embedded firewalls and intrusion detection system.
  - SIPRNET and NIPRNET (local area network). Routers include embedded intrusion detection system modules.
- **High assurance IP encryption.** Encrypts and decrypts SIPRNET and NIPRNET traffic for transmission over the wide-area network. The plain text side connects to SIPRNET and NIPRNET switches; the cipher text side connects to the colorless router.
- **Satellite communications on-the-move.** The roof-mounted satellite communications antenna uses Global Positioning System data and the inertial navigation system to track geostationary Ku or Ka band communications satellites while on-the-move.
- **User access interface.** Two user access cases (SIPRNET and NIPRNET) with uninterruptible power supplies. The user access cases provide digital and analog voice and digital data subscriber access ports for users at static command posts. Each user access case provides 48 Ethernet ports and 24 2-wire analog telephone ports. The user access cases have no transmission capabilities, so the TCN provides their network transport.

- **Redundant Power.**
  - An on-board 15-kilowatt diesel generator supports operations while on-the-move.
  - Either the towed, 30-kilowatt generator or utility power provides prime power while at-the-halt.

POINT OF PRESENCE

2-48. A Point of Presence provides access to the DODIN-A 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.

2-49. 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 division. When operating at-the-halt, the Point of Presence can provide access for wired IP data terminals or SIPRNET VoIP phones. On-the-move, it provides the same capabilities to users on-board the vehicle.

2-50. Network planners configure Point of Presence components before deployment. The network management subsystem can dynamically update subsequent configurations over-the-air.

SIPRNET and Colorless Enclaves

2-51. The Point of Presence supports the SIPRNET and colorless security enclaves. Users operate in the SIPRNET enclave. There are no user connections directly to the colorless core. The Point of Presence uses software call management for local call control.

Point of Presence Services

2-52. Point of Presence network services include—

- **Mission command information systems and applications.**
  - Tactical Ground Reporting.
  - Command Post of the Future.
  - Virtual network computing compatibility with Force XXI Battle Command, Brigade and Below; Joint Combat Radio; and Joint Battle Command-Platform.
- **Quality of service:** The Point of Presence provides quality of service assurance for the SIPRNET local area network using differentiated services code point marking. Differentiated services provide low latency for traffic that cannot handle delayed transmission, such as VoIP and video teleconferencing. A quality of service edge device provides measurement-based admission control and network preemption to ensure the amount of traffic does not exceed the network's ability to support.
- **Information services on the SIPRNET local area network—**
  - Domain Name System.
  - Dynamic Host Configuration Protocol.
  - Active Directory.
- **Cybersecurity:** The Point of Presence provides multiple layers of cybersecurity protection—
  - TACLANEs encrypt SIPRNET data for communications security protection on the Highband Networking Radio and satellite communications links.
  - The colorless and SIPRNET routers provide enclave-level transmission security protection and physical separation between security enclaves.
  - The distributed computing element and Soldier Kiosk use cybersecurity software for additional layers of defense-in-depth.
  - Common access card readers enable identity and access management.
- **Local node management:** Operators perform basic fault isolation based on power on self-test results and other diagnostics.

  - The Node Management Subsystem monitors, and manages local SIPRNET services, devices, and interfaces.
  - The Local Area Network Management Subsystem monitors, and manages SIPRNET local area network hosts, devices, and interfaces.
- **Call control:** The Point of Presence uses software call management for SIPRNET voice call control. The call management software provides—
  - Call processing.
  - Call forwarding.
  - Call transfer.
  - Redial.
- **Conference bridging:** The Point of Presence provides a nonsecure conference bridge for multi-party voice calls and progressive conferencing.

Transmission Technologies Supported

2-53. The Point of Presence supports both line of sight and satellite communications while on-the-move and at-the-halt. Both the terrestrial Highband Networking Radio and satellite communications network centric waveform require position information to operate, whether at-the-halt or on-the-move. The inertial navigation unit and the Global Positioning System receiver provide this position data. The Point of Presence also provides this position data for the map-based monitoring function of the NOSC's network management system.

Line of Sight Communications

2-54. The Highband Networking Radio provides the Point of Presence with bandwidth-on-demand. It uses a C band antenna to transmit and receive the highband networking waveform at-the-halt and on-the-move.

2-55. The Highband Networking Radio continuously scans for other Highband Networking Radios within range. When one radio detects another, it establishes a connection, or relationship. This creates a network to forward data from the source to the target destination.

2-56. Neighboring radios forward calls to provide alternate communication paths. A neighbor in this case is another platform using a Highband Networking Radio. This forms a mesh network. The Highband Networking Radio functions in peer-to-peer and point-to-multipoint modes.

Satellite Communications

2-57. The Point of Presence employs a time division multiple access satellite communications link using either commercial Ku band or military Ka band. The network management system automatically switches between line of sight and satellite communications transport as needed to provide uninterrupted service using the better connection.

Employment

2-58. Points of Presence at the division, brigade and battalion levels provide wide-area network connections to enable command and control and staff collaboration while on-the-move and at-the-halt. Points of Presence can also provide high data rate user connections for wired IP data terminals or VoIP phones at the quick halt and at-the-halt to support command post operations.

2-59. The commander's Point of Presence hosts command and control-enabling applications and services to facilitate situational understanding while on-the-move. Commanders can use the Point of Presence to monitor activities in their area of operations via Command Post of the Future or chat applications while on-the-move or during command post displacement.

2-60. The assistant chief of staff, operations (G-3) or battalion or brigade operations staff officer (S-3) Point of Presence enables continuous staff coordination and planning while on-the-move, at the quick halt, and during command post displacement.

SOLDIER NETWORK EXTENSION

2-61. The Soldier Network Extension can operate installed in a variety of command vehicles at battalion and company levels. It provides either Ku or Ka band satellite communications on-the-move. The Soldier Network Extension provides reach between brigade combat teams, and reachback communications to the division. It supports company commanders and selected platoon leaders in maneuver battalions. The communications traffic served includes command and control messages, voice calls, and situational understanding information.

2-62. The Soldier Network Extension can serve as an access port to extend the range of legacy combat net radios. This makes these networks more robust. The combat net radio gateway can connect two different radio networks to the WIN-T IP infrastructure. WIN-T satellite communications capabilities effectively extend the range of the radio network beyond line of sight. The combat net radio gateway provides telephone signaling and converts analog voice to digital data. The Soldier Network Extension is a general-purpose user-operated system not supported by dedicated signal manning.

2-63. Antenna position information from the Global Positioning System receiver helps maintain antenna pointing. The position information also supports the map-based monitoring function of the NOSC's network management system.

SIPRNET and Colorless Enclaves

2-64. The Soldier Network Extension supports the colorless and SIPRNET security enclaves. All wide-area network traffic to and from a Soldier Network Extension passes through the colorless enclave. There are no user connections directly to the colorless core; users operate in the SIPRNET enclave. The Soldier Network Extension uses software call management for local call control

Soldier Network Extension Services

2-65. Soldier Network Extension network services include—

- **Mission command information systems and applications.**
  - Tactical Ground Reporting.
  - Virtual network computing compatibility with Force XXI Battle Command, Brigade and Below; Joint Combat Radio; and Joint Battle Command-Platform.
- **Quality of service:** The Soldier Network Extension provides quality of service assurance for the SIPRNET local area network using differentiated services code point marking. Differentiated services provide low latency for traffic that cannot handle delayed transmission, such as VoIP and video teleconferencing. A quality of service edge device provides measurement-based admission control and network preemption to ensure the amount of traffic does not exceed the network's ability to support.
- **Information services on the SIPRNET local area network—**
  - Domain Name System.
  - Dynamic Host Configuration Protocol.
  - Active Directory.
- **Cybersecurity:** The Soldier Network Extension provides multiple layers of cybersecurity protection—
  - TACLANEs encrypt SIPRNET data for communications security protection over the satellite communications link.
  - Colorless and SIPRNET routers provide enclave-level transmission security protection.
  - The distributed computing element and Soldier Kiosk use cybersecurity software for additional layers of defense-in-depth.
  - Common access card readers enable identity and access management.
- **Local node management:** Operators perform basic fault isolation based on power-on self-test results and other diagnostics.

  - The node management subsystem monitors and manages local SIPRNET services, devices, and interfaces.
  - The local area network management subsystem monitors and manages SIPRNET local area network hosts, devices, and interfaces.
- **Call control:** The Soldier Network Extension uses software call management for SIPRNET voice call control. The call management software provides—
  - Call processing.
  - Call forwarding.
  - Call transfer.
  - Redial.
- **Conference Bridging:** The Soldier Network Extension provides a nonsecure conference bridge for multi-party voice calls and progressive conferencing.

Transmission Technologies Supported

2-66. The Soldier Network Extension uses either Ku or Ka band satellite communications on-the-move and at-the-halt. The combat net radio gateway connects single-channel radio networks to the WIN-T IP network.

Employment

2-67. The Soldier Network Extension serves different roles within the formation, depending on where it is allocated. The Soldier Network Extension at the battalion S-3 section enables continuous staff coordination while on-the-move and at the quick halt.

2-68. The field artillery battalion fire direction center Soldier Network Extension enables fires coordination and maintains awareness and system connectivity while fire direction centers displace. The system allows positioning of firing batteries and fire direction centers wherever the commander needs without the constraints of fixed line of sight transmission. This allows faster displacement of fire direction centers following counterfire missions

2-69. The Soldier Network Extensions in the brigade and battalion retransmission teams extend or expand network range, interconnectivity, and capacity. The combat net radio gateway can extend one combat net radio voice network over the wide-area network to extend network range across a large or non-contiguous operational area.

TACTICAL RELAY-TOWER

2-70. 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 either as a standalone unit or in conjunction with a colocated TCN. 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 highband networking waveform over the colorless enclave. The Tactical Relay-Tower provides no networking capabilities or user services for either SIPRNET or NIPRNET.

2-71. The Tactical Relay-Tower transmission subsystem consists of a Highband Networking Radio for high-throughput ground-to-ground communications with other Highband Networking Radios. It operates as part of a mobile, ad hoc network. The radio uses time division duplex/time division multiple access networking to provide bandwidth-on-demand. The Tactical Relay-Tower uses two antennas—the Highband Radio Frequency Unit-C band antenna and the directional Range Throughput Extension Kit panel antenna.

2-72. The trailer-mounted Global Positioning System input/output block and the inertial navigation unit at the top of the antenna mast provide position and timing information. The antennas and network management system use the positioning information for distance calculation and antenna direction adjustments.

2-73. The Tactical Relay-Tower requires a line of sight path to the other end of the intended link. Pre-planned mission scenarios, used in conjunction with maps, reports, and other information, assist in site selection

during mission planning. Planners should consider obstructions such as terrain, foliage, and buildings when developing these scenarios.

2-74. Planners and operators should set up the Tactical Relay-Tower away from aircraft runways and heliports. Planners need to coordinate with the installation airfield/airspace officer or, in a combat zone, the senior airfield authority. The aircraft warning beacons on the antenna mast should be installed, operational, and used, if the mission permits. During nighttime operations, the aircraft warning beacons can be switched to infrared operation to allow safe flight operations while maintaining light discipline.

NETWORK OPERATIONS AND SECURITY CENTER

2-75. The WIN-T NOSCs include subsystems for network planning, administration, monitoring, and response in the SIPRNET, NIPRNET, and colorless enclaves. The NOSCs include external modular command post facilities to support the G-6 (S-6) staffs. WIN-T increment 2 includes two versions of the NOSC—the NOSC-Division, and the NOSC-Brigade. Soldiers at the NOSCs conduct DODIN operations in their corresponding portions of the network. The NOSC provides monitoring and DODIN operations capabilities in the colorless, SIPRNET, and NIPRNET enclaves—

- **Colorless**
  - Wide-area network management.
  - Network management.
  - Virtual machine management.
- **SIPRNET**
  - Cybersecurity device management.
  - Wide-area network management.
  - WIN-T network management.
  - Key management.
  - Virtual machine management.
  - Inline network encryptor management.
  - Service desk management.
  - Desktop configuration management.
  - Spectrum planning (refer to ATP 6-02.70).
  - Network management.
- **NIPRNET**
  - Cybersecurity device management.
  - Wide-area network management.
  - Operations management.
  - Event monitoring.
  - Performance tracking.
  - Security policy enforcement.
  - Audit capability.
  - WIN-T network management.
  - Inline network encryptor management.
  - Service desk management.
  - Desktop configuration management.
  - Network client management.

2-76. The NOSC is equipped with SIPRNET, NIPRNET, and colorless access cases with uninterruptible power supplies to monitor and manage their respective enclaves while at-the-halt. The SIPRNET and NIPRNET user access cases provide digital voice, analog voice, and digital data subscriber access ports for users at static command posts. Each user access case provides 48 Ethernet ports and 24 2-wire analog telephone ports. User access cases have no transmission capabilities.

2-77. The NOSC uses a TCN for network connectivity. The TCN routes data between network devices, network links, and the NOSC. This allows the NOSC to monitor network status. Soldiers at the NOSC analyze status information so they can effectively mitigate adverse events on network devices or links.

COMMUNICATIONS AND NODE MANAGEMENT CAPABILITIES

2-78. The various WIN-T increment 2 node types provide communications and node management capabilities at-the-halt and on-the-move using line of sight, satellite communications, and IP networking technology. Table 2-1 provides a summary of increment 2 nodes' communications and node management capabilities.

Table 2-1. Increment 2 communications and node management capabilities

Node Type	*Network Centric Waveform (SATCOM)*	*Frequency Division Multiple Access (SATCOM)*	*Highband Networking Radio (line of sight)*	*Combat Net Radio Gateway*	*Local Node Management*	*Soldier Kiosk*	*DISN Services*
TCN	X	—	X	X	X	X	X
POP	X	—	X	—	X	—	X
SNE	X	—	—	X	X	—	X
NOSC	—	—	—	—	X	—	—
THN	X	X	—	—	X	—	—
TR-T	—	—	X	—	—	—	—
STT	X	X	—	—	—	—	—

Legend:

DISN	Defense Information Systems Network	STT	Satellite Transportable Terminal
NOSC	Network Operations and Security Center	TCN	Tactical Communications Node
POP	Point of Presence	THN	tactical hub node
SATCOM	satellite communications	TR-T	Tactical Relay-Tower
SNE	Soldier Network Extension		

INCREMENT 1B

2-79. WIN-T increment 1b operates at-the-halt only. WIN-T increment 1b system allocation within the corps, Reserve Component division, multifunctional support brigade, expeditionary signal company, and joint/area signal company uses standardized system configurations, according to the function and echelon of the unit. Increment 1b uses line of sight and satellite communications network transport and, delivers user services through the tactical hub node, Joint Network Node, and Command Post Node.

JOINT NETWORK NODE

2-80. The Joint Network Node is a vehicle-mounted communications platform that extends information services and provides node management and prioritization. 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 DISN services.

2-81. The Joint Network Node connects users to SIPRNET, NIPRNET, secure and nonsecure analog phones, secure VoIP 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.

2-82. The Joint Network Node backbone connection to the regional hub node uses a dedicated frequency division multiple access satellite communications link. The Joint Network node shares bandwidth among Command Post Nodes using network centric waveform satellite communications.

2-83. Joint Network Node capabilities include—

- **SIPRNET and NIPRNET VoIP call control.** Includes call forwarding, call transfer, redial, and conference bridging.
- **DISN services.** SIPRNET, NIPRNET, and top secret sensitive compartmented information.
- **Video teleconferencing.** Classified and non-classified.
- **Private branch exchange service.** Analog telephone service.
- **Enclave boundary protection.** Tier 2 perimeter router.
- **Colorless core.** Cryptographically isolated SIPRNET, NIPRNET, and sensitive compartmented information networks.
- **Ethernet switching.** SIPRNET and NIPRNET local area networks with power over Ethernet for IP phones.
- **Fiber optic interface.** A multi-channel, synchronous time division digital multiplexer and fiber optic modem with tactical fiber optic cable assembly connections to line of sight and satellite communications transport systems.
- **Transport interfaces.** Can interface with Satellite Transportable Terminal, high capacity line of sight, Phoenix satellite communications terminal, or SMART-T for alternate network transport capabilities.
- **Redundant Power.** Provided by either towed 10-kilowatt generator or utility power.

COMMAND POST NODE

2-84. The Command Post Node provides SIPRNET, NIPRNET, secure and nonsecure VoIP, and battlefield video teleconferencing services. Command Post Nodes support battalion command posts at-the-halt. 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.

2-85. The battalion S-6 controls network services from the command post. The battalion supplies its own automated information systems and telephone equipment. The supported battalion sets up and operates this equipment with technical oversight from their S-6.

2-86. Command Post Node capabilities include—

- **SIPRNET and NIPRNET VoIP call control.** Includes call forwarding, call transfer, redial, and conference bridging.
- **DISN services.** SIPRNET and NIPRNET.
- **Video teleconferencing.** Classified and non-classified.
- **Colorless core.** Cryptographically isolated SIPRNET and NIPRNET.
- **Alternate transport.** Can interface with Satellite Transportable Terminal, high capacity line of sight, Phoenix satellite communications terminal, or SMART-T for alternate network transport capabilities.
- **Redundant Power.** Provided by either towed 10-kilowatt generator or utility power.

COMMUNICATIONS AND NODE MANAGEMENT CAPABILITIES

2-87. The various WIN-T increment 1b node types provide communications and node management capabilities at-the-halt using line of sight, satellite communications, and network management technologies. Table 2-2 on page 2-17, provides a summary of increment 1b nodes' communications and node management capabilities.

Table 2-2. Increment 1b communications and node management capabilities

Node Type	*Network Centric Waveform (SATCOM)*	*Frequency division multiple access (SATCOM)*	*Line of sight transport*	*Node management*	*DISN services*
Tactical hub node	X	X	—	X	X
Joint Network Node	—	—	—	X	X
Command Post Node	—	—	—	—	X
Satellite Transportable Terminal	X	X	—	X	—
High capacity line of sight	—	—	X	—	—
Commercial coalition equipment	—	—	—	—	X
Modular Communications Node-Enhanced Enclave	—	—	—	—	X
Legend:					
DISN	Defense Information Systems Network				
SATCOM	satellite communications				

This page intentionally left blank.

Chapter 3
Managing the Tactical Network

This chapter introduces management of the tactical network. It discusses Department of Defense information network operations (including cybersecurity), network operations and security centers, and node management functions and tools. It also addresses planning, configuring, and setting data priorities for quality of service and speed of service assurance so the network can support the commander's intent.

DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS

3-1. DODIN operations capabilities enable the signal staffs at each echelon to execute commanders' priorities throughout the enterprise. DODIN operations allow commanders to use automated information systems to effectively communicate, collaborate, share, manage, and disseminate information. DODIN operations consist of three critical tasks—

- Enterprise management.
- Cybersecurity.
- Content management.

3-2. Shared network situational understanding, along with coordination between stakeholders on network events, ensures commanders are aware of network actions in their areas of operation and enables them to manage their portions of the network as they would other combat systems. The division and brigade NOSCs perform DODIN operations for the upper tier tactical internet. Battalions perform DODIN operations for the lower tier tactical internet. Refer to ATP 6-02.53 for more information about DODIN operations in the lower tier tactical internet.

3-3. WIN-T uses commercial firewalls, network planning and management tools, and cybersecurity techniques as a framework for network defense-in-depth. Increment 2 extends the defense-in-depth approach, and integrates network management into the architecture. Refer to ATP 6-02.71 for more detailed information on the DODIN operations critical tasks.

ENTERPRISE MANAGEMENT

3-4. DODIN enterprise management is the technology, processes, and policies necessary to install, operate, maintain, and sustain effective communications networks, information systems, and applications. DODIN enterprise management merges IT services with DODIN operations critical capabilities (ATP 6-02.71). Enterprise management consists of five functional services:

- Enterprise systems management.
- Systems management.
- Network management.
- Satellite communications management.
- Frequency assignment.

Enterprise Systems Management

3-5. Enterprise systems management focuses on end-user and system applications focuses on the availability, performance, and responsiveness of enterprise services. Enterprise services include—

- DOD Enterprise E-mail.
- DOD Enterprise Portal Service.
- Defense Collaboration Services.
- Enterprise search.
- Enterprise file share.
- Identity and access management.

Systems Management

3-6. Systems management provides day-to-day administration of computer-based systems, elements of systems, and services including software applications, operating systems, databases, and hosts of end-users. Systems management is comprised of all measures necessary to operate enterprise systems and services effectively and efficiently (ATP 6-02.71).

Network Management

3-7. Network management provides a network infrastructure with the desired level of quality and assured service. Networks included in enterprise management are located on all transmission media and tiers of communication: terrestrial, aerial, and satellite communications.

Satellite Communications Management

3-8. Satellite communications management is the day-to-day operational control of satellite communications resources. Refer to ATP 6-02.54 for more information about satellite communications management.

Frequency Assignment

3-9. Frequency assignment involves ensuring electromagnetic spectrum resources are available to support effective and efficient frequency use for the wireless portion of the network. The electromagnetic spectrum manager manages frequency assignments and coordinates spectrum use with the electronic warfare section. Refer to ATP 6-02.70 for more information about spectrum management.

CYBERSECURITY

3-10. The Army depends on reliable networks and systems to access critical information and supporting information services to accomplish their missions. Threats to the DODIN-A exploit the increased complexity and connectivity of Army information systems and place Army forces at risk. Like other operational risks, cyberspace risks affect mission accomplishment. 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.

3-11. Multi-layer cybersecurity protection maintains the integrity of both the network and the information passing through it. WIN-T secures the network consistent with the classification of information passed over the network. The cybersecurity architecture allows G-6 and S-6 network leaders to make informed risk decisions and effectively defend network resources. Refer to ATP 6-02.71 for more information about the cybersecurity framework. Refer to DODI 8510.01 for more information about the DOD risk management framework.

Network Defense-in-Depth

3-12. *Defense-in-Depth* is an information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization (CNSSI 4009). WIN-T cybersecurity protection integrates network defense-in-depth, starting at the DISN and

extending to the local area networks and individual user devices. In addition to the encrypted IP backbone, the defense-in-depth approach implements robust cybersecurity protection throughout the network. This layers protection at the outer perimeter and further downstream at the local area networks. Cybersecurity measures implemented at the servers and laptops provide an additional layer of protection. These protection mechanisms use commercial off-the-shelf cybersecurity hardware and software for—

- Firewalls.
- Anti-virus detection and blocking.
- Intrusion detection.
- Malicious mobile code detection
- Identity and access management.

Risk Management Framework

3-13. The DOD risk management framework (formerly the DOD Information Assurance Certification and Accreditation Process) provides a disciplined and structured process for combining information systems security and risk management into the system development life cycle. The DOD risk management framework complies with National Institute of Standards and Technology guidelines to align with federal civilian agencies. The six steps of the risk management framework are—

- Categorize the system.
- Select security controls.
- Implement security controls.
- Assess security controls.
- Authorize system.
- Monitor security controls.

3-14. Because a security vulnerability to one system places the entire network at risk, it is important to exercise due diligence in the risk management framework. Refer to DODI 8510.01 for details about applying the DOD risk management framework.

Administering Cybersecurity Policies

3-15. Cybersecurity policies and procedures identify security guidelines for data, media, telecommunications equipment, and information systems. These policies and procedures also help ensure the confidentiality, integrity, and availability of the users' systems and data. Strict adherence to cybersecurity policies helps maintain a hardened network perimeter.

CONTENT MANAGEMENT

3-16. Content management, comprised of information dissemination management and content staging, manages access to, and delivery of, relevant, accurate information to the appropriate users promptly, efficiently, and in the proper format. For the Army, content management activities are information dissemination management and content staging. Refer to ATP 6-02.71 for more information about information dissemination management and content staging.

NETWORK OPERATIONS AND SECURITY CENTERS

3-17. The division and brigade NOSCs perform network planning, monitoring, administration, and reporting. Network planners, operators, maintainers, and technicians in the NOSCs—

- **Plan for networks and devices:** develop and maintain both high-level and in-depth layouts and plans for DODIN operations, including detailed configuration files for most devices.
- **Adjust plans as needed:** relay changes and updates where required.
- **Monitor networks:** collect and report the status of the network. The interpretation of the status prompts anomaly response. Either the NOSC or a managed element, such as a TCN, may initiate this response.

- **Manage user profiles:** control user profiles to ensure all users share a common network configuration. This reduces the number of network environment-related problems.
- **Perform network management activities:** monitor the performance of network assets, including media. This includes updating software versions and virus definitions, and troubleshooting to mitigate network and device problems. The goal is continuous, effective network performance.

NETWORK OPERATIONS AND SECURITY CENTER EQUIPMENT

3-18. The NOSCs contain computer servers, Ethernet switches, and network appliances dedicated to planning and managing the SIPRNET, NIPRNET, and colorless enclaves. During operation, shelter-mounted assets remain in the truck. The SIPRNET, NIPRNET, and colorless user access cases operate in a unit-provided command post at-the-halt. The remote laptops communicate with the shelter-mounted servers and other networking assets.

3-19. The Ethernet switches in the shelter and in the user access cases have twin Gigabit Ethernet ports. At the shelter Ethernet switch, one port provides a high-throughput link between the NOSC assets and the user access cases supporting the remote management laptops in the command post. The second port provides a high-throughput connection to the TCN. This link allows the NOSC to access extended network assets, providing both a path for status reporting and a link for managing configurations and operating policies. The tactical fiber optic cable assembly provides the Gigabit Ethernet connections to the TCN and the command post.

3-20. The brigade NOSC is subordinate to the division NOSC in operations, and performs DODIN operations for the brigade's portion of the network. The brigade NOSC is scaled to the brigade's DODIN operations mission, and lacks some of the traffic analysis and network diagnostics capabilities resident at the division NOSC.

NETWORK MANAGEMENT FUNCTIONS

3-21. Typical management functions include—

- Monitoring the network, including map-based monitoring of at-the-halt and on-the-move nodes.
- Implementing distributed node management.
- Administering cybersecurity policies.
- Managing cryptographic keys and public key infrastructure.
- Managing quality of service.
- Correlating network and device events and predicting trends to avoid problems.
- Managing network topology and administering cybersecurity policies.
- Planning spectrum use for all known emitters and managing friendly network emitters (refer to ATP 6-02.70).
- Coordinating satellite access requests with the applicable regional satellite communications support center and ensuring all satellite terminals in the network operate in accordance with the assigned satellite access authorization.

3-22. Soldiers at the NOSC manage device configurations and network architecture for multiple types of communications equipment. They manage constantly changing networks and maintain gateways to external networks. The NOSC provides tools capable of monitoring and managing networks using multiple line of sight and satellite communications links to communicate over an extended area.

3-23. The NOSC provides updated information to the networking components, including—

- Configuration files.
- Virus definition updates.
- Cybersecurity updates.
- Communications goals.
- Network policies.

3-24. Network nodes collect local device and network link status. They provide it to the NOSC via the TCN.

NETWORK OPERATIONS AND SECURITY CENTER SOFTWARE

3-25. Various software applications support the NOSC functions. These applications fall into one of three categories—

- Operating systems.
- Network management software.
- Network operations software.

Operating Systems

3-26. An operating system is a collection of software that manages computer hardware resources and provides common services to execute application software. All servers and laptops have underlying operating systems to manage their internal resources. Networking appliances, such as routers and switches, also require operating systems to manage their hardware.

Network Management Software

3-27. This category includes software applications developed specifically to support WIN-T, including—

- Network planning software.
- Wide-area network monitoring software.
- Node management software.
- Key management software.
- In-line encryptor management software.

Network Operations Software

3-28. The WIN-T network management system uses a combination of government off-the-shelf and commercial off-the-shelf software applications. These software applications automate and simplify many of the functions required to plan and manage the deployed communications network.

Government Off-the-Shelf

3-29. These are preexisting, government-owned applications developed to fulfill specific requirements for one or more government agencies. Government off-the-shelf network operations applications include—

- Automated Communications Engineering Software.
- Spectrum XXI spectrum management software.
- Common access card middleware.
- Radiant Mercury (cross-domain solution software).

Commercial Off-the-Shelf

3-30. WIN-T uses the same types of commercial applications used to manage mid-sized to large networks in commercial and business settings, where applicable. Popular software applications in this group include—

- Application and server management software.
- Network monitoring applications.
- Anti-virus and spyware applications.
- Centralized security management applications.

PLANNING TACTICAL NETWORKS

3-31. At a NOSC, senior network planners typically develop network plans from strategic concept to tactical implementation, including the resources, device and network configurations, and operational policies to develop and maintain networks and services. Their efforts support division and brigade combat team operations.

3-32. A network planner can graphically model, plan, define and configure network assets for both at-the-halt and on-the-move employment. The graphical planning applications support configuring nodes, units, antennas, satellite communications bandwidth, and radios. Planning also includes—

- On-the-move node planning.
- Local access waveform radios.
- Highband Networking Radios.
- Network centric waveform modems.
- High capacity line of sight radios.
- Frequency division multiple access satellite communications planning.
- Combat net radio planning (single-channel ground and airborne radio system and Enhanced Position Location Reporting System) (refer to ATP 6-02.53).
- Quality of service planning.
- IP and router planning.
- Voice service planning.
- Spectrum planning for all known emitters and management of network emitters (ATP 6-02.70).
- Cybersecurity planning.
- Address book planning.

SATELLITE COMMUNICATIONS PLANNING

3-33. For WIN-T increment 1b, planners generate a satellite access request for each satellite transportable terminal and the tactical hub node, if used. For increment 2, planners submit satellite access requests for—

- Division main command post:
  - Satellite Transportable Terminal—frequency division multiple access and network centric waveform.
  - TCN—network centric waveform.
  - Tactical hub node, if used—frequency division multiple access and network centric waveform.
  - SMART-T (to higher headquarters).
- Division tactical command post:
  - Satellite Transportable Terminal—frequency division multiple access and network centric waveform.
  - TCN—network centric waveform.
- Brigade main command post:
  - Satellite Transportable Terminal—frequency division multiple access and network centric waveform.
  - TCN—network centric waveform.
  - SMART-T (to higher headquarters).
- Brigade tactical command post:
  - Satellite Transportable Terminal—frequency division multiple access and network centric waveform.
  - TCN—network centric waveform.
- Battalion command post:
  - Satellite Transportable Terminal—network centric waveform.
  - TCN—network centric waveform.
- Point of presence—network centric waveform.
- Soldier network extension—network centric waveform.

3-34. The network management technician normally oversees the satellite access request submission process. The satellite communications planner compiles the required information and provides it to the

spectrum manager for entry into the Army Centralized Army Service Request System or the Joint Integrated Satellite Communications Tool (SIPRNET). Refer to ATP 6-02.54 for more information about satellite communications planning.

REGIONAL HUB NODE COORDINATION

3-35. Planners should conduct several coordination calls leading up to each exercise or mission that uses the regional hub node for access to the DODIN-A and DISN services. This ensures the regional hub node can adequately support mission intent. 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.

3-36. Units may choose to provide a liaison to the regional hub node during the installation of the WIN-T network, or for the duration of the mission. While not necessary, a liaison can assist communicating a deployed unit's status and connectivity issues.

3-37. The United States Army Communications-Electronics Command provides regional hub node playbooks as technical guides to support installation and troubleshooting. The regional hub node playbooks are available at the Army Centralized Army Service Request System Website.

ESTABLISHING TACTICAL NETWORKS

3-38. The WIN-T network is largely self-forming after equipment initialization, network planners and operators must accomplish certain tasks to establish and secure the network. After establishing the network, operators must ensure all forms of cybersecurity protection function according to the network cybersecurity policies.

3-39. Operators should record normal operating system parameters and system settings for future use, these parameters assist in identifying network congestion and developing problems. These operating parameters provide a baseline to configure equipment after removal for maintenance.

PRIORITIES OF WORK

3-40. Standard operating procedures generally dictate unit priorities of work. However, the commander may change the priorities of work based on the mission variables. If there are not enough Soldiers available to perform all of the tasks associated with setting up a command post and site security, priorities can change to accomplish the most important task first. Clear priorities of work ensure personnel complete key tasks necessary to establish the network and command post capabilities first. Signal leaders continuously supervise the setup of communications systems to ensure crews follow the priorities of work.

3-41. Leaders should establish clear priorities of work for all operators and all systems. Defining clear priorities increases a team's efficiency in accomplishing assigned tasks, reduces Soldier idle time and maintains focus on mission requirements and link establishment.

3-42. 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 (S-6) priorities must support the G-3 (S-3) and commander's priorities. Figure 3-1 on page 3-8, shows a sample table for link establishment priorities.

CODE

LINK CODE	
SX	Satellite
FL	Fiber
L	LOS
CX	Cable

SF=FDMA, ST=TMDA, SM=SMART-T
FT=TFOCA, FS=Single Mode, FM=Multimode
LH=HCLOS, LI=IPLOS
CC=CatV, CX=CX11230

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, 72, 75, 76, 77		
1	ST75	00, 47, 48, 72, 72, 75, 76, 77		
1	ST76	00, 47, 48, 72, 72, 75, 75, 77		
1	ST77	00, 47, 48, 72, 73, 74, 75, 76		
2	SF4700	0		JNN FDMA connectivity to hub.
2	SF4800	0		JNN HCLOS backbone.
3	LH4748	48		
3	LH4847	47		CPN 7745 fiber link to 7747.
4	FT4775	75		JNN SMART-T redundant links to each other.
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 mutiple 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 mutiple access
TFOCA	tactical fiber optic cable assembly

Figure 3-1. Sample link establishment priorities

PORT SECURITY

3-43. Port security prevents unauthorized access to the network. Unused switch ports should be disabled or configured in a parking (un-routable) virtual local area network. Network administrators should add new users manually. Port security could entail using persistent medium access control (MAC) address learning (sticky MAC) and MAC limiting. With sticky MAC and MAC limiting enabled, switch interfaces can learn the MAC addresses of trusted workstations, phones, and servers until they reach their limits for MAC addresses. Once a device reaches its MAC address limit, it denies any new devices on the switch, even after a switch restart. Administrators can also implement a MAC table with a list of approved devices so known systems can connect to the network while preventing access using unauthorized devices.

3-44. Dynamic Host Configuration Protocol can simplify and speed command post initialization, since automation personnel do not need to manually configure and add each user to the switch. However, using Dynamic Host Configuration Protocol during normal operation creates an opportunity for unknown users to connect to the network. For this reason, network managers should disable Dynamic Host Configuration

Protocol and implement port security as soon as the digital command post footprint and primary users are established.

WIDE-AREA NETWORK AND LOCAL AREA NETWORK DIAGRAMS

3-45. Wide-area network and local area network diagrams provide visual representations of network topology on both the wide-area network and local area network. Accurate network diagrams simplify network troubleshooting and aid in planning for potential network growth. Network diagrams are also effective briefing tools, since they make the network topology much easier to visualize.

3-46. DODIN operations personnel should produce wide-area network and local area network diagrams for each training event. DODIN operations personnel update local and wide-area network diagrams continually to show network changes.

- Wide-area network diagrams should depict—
  - Each node, with node identification number.
  - Node location.
  - Assemblages.
  - Each wide-area network link—satellite communications, line of sight, or cabled.
  - Non-organic elements.
- Local area network diagrams should identify—
  - All access cases.
  - Separate switches.
  - Port count.
  - Loopback IP addresses.
  - Physical locations inside command post tents or buildings.
  - Supported users.

MAINTAINING TACTICAL NETWORKS

3-47. The two major functions in maintaining a network are network management and network monitoring. Network management implies active responses to known issues. Network monitoring gauges the health of network assets based on the status information those assets report to the NOSC. Monitoring is a subordinate function to network management.

SIMPLE NETWORK MANAGEMENT PROTOCOL MANAGEMENT

3-48. The WIN-T NOSCs use SNMPc software to monitor the network infrastructure in near real-time. SNMPc is WIN-T's primary network management tool. Network managers should configure SNMPc maps to monitor network devices, links, and services.

3-49. Network managers should configure SNMPc to poll networking devices using loopback IP addresses, and links using the open shortest path first neighbor relationship to the adjacent router. SNMPc should also poll servers periodically to ensure services are still available. For example, domain name system server port 53, Exchange port 25, and Command Post of the Future Ventrilo port 3784.

3-50. SNMPc OnLine provides the signal company commander, S-3, G-6 (S-6), and command post a read-only view of the network. This allows remote viewing of Simple Network Management Protocol maps using a web browser to provide near real-time network status. This allows the commander, S-3, and G-6 (S-6) to monitor the network, and facilitates status briefings.

3-51. Simple Network Management Protocol manager to manager communication allows battalions to remotely view the brigade network, and the brigade to view the division or an adjacent brigade network. This creates an SNMPc icon on each management console that provides a read-only view when selected. Using manager to manager communication reduces network management overhead by providing the current network status without polling the individual network devices.

3-52. Asynchronous monitoring, using Simple Network Management Protocol traps, alerts DODIN operations personnel to critical events. Monitoring the router's central processing unit and memory utilization with traps can identify potential network or hardware problems, such as bad routing, network convergence, or multicast broadcast storms that increase central processing unit and memory utilization. Environmental (fan and temperature) traps provide alerts if network devices overheat, or are in danger of overheating.

3-53. The Simple Network Management Protocol community string on routers, switches, and firewalls transmits in clear text. Network managers should change the default community string as they would a password so attackers cannot exploit this weakness to gain network access.

INTERNET PROTOCOL MANAGEMENT

3-54. IP management is essential to planning, managing, and tracking assigned IP addresses. During planning, it is critical to identify where specific systems are located logically, and identify specific subnets associated to devices within the planned network architecture. 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.

3-55. IP address planning 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 (when using installation as a docking station) and the regional or tactical hub node to avoid dual advertisement.

3-56. An IP address database tracks used, reserved, allocated, and free IP addresses. This presents a clear picture of IP address usage within the organization. An accurate database prevents fragmented IP address usage and allows network planners to take necessary actions before allocations run out. Comparing the inventory database with the established network identifies network discrepancies and helps track allocated IP space. DODIN operations personnel should periodically compare the established network with the IP database. The use of automated IP discovery tools speeds up the process and improves the accuracy of inventories.

3-57. IP management tracking correlates computers and network devices with their physical locations and users. This helps DODIN operations personnel to rapidly identify, locate, and remediate compromised systems and assists in identifying cybersecurity events or violations.

PASSWORD MANAGEMENT

3-58. Proper password management is a key to network security, since compromised or easily guessed passwords can grant unauthorized users unrestricted access to the network. Units should use centrally managed password management systems, for example, RADIUS or Terminal Access Controller Access Control System. Users require individual logins for each system and role, using strong passwords according to Army password standards. User accounts with system-level privileges require a separate password from all other accounts held by that user.

3-59. Using default passwords on networking devices or consoles presents a significant network vulnerability. Army password standards require changing the passwords on routers and system consoles from the factory default. This includes changing from the default passwords provided by the program manager during equipment fielding. Since default passwords are widely known, adversaries or opposing forces in their attempts to infiltrate the network, try them first.

3-60. All system or system-level privileged-level accounts—root, enable, and administration accounts—require at least a 15-character case-sensitive password, changed every 60 days. Refer to Army Information Assurance Best Business Practices Document 04-IA-O-0001 for additional password requirements.

FIREWALL MANAGEMENT

3-61. Effective firewall management requires understanding of—

- The Lightweight Directory Access Protocol Data Interchange Format.

- IP management.
- The ports, protocols, and services management system.

3-62. DODIN operations personnel need to know where their organic IPs are located, both physically and logically in the network, and which IPs to allow access from outside the local area network. They also need to configure ports, protocols, and services for mission command information systems and other authorized automated information system software.

3-63. The default firewall configuration uses a block by exception rule set. Block by exception allows the vast majority of outside traffic to access the network. Managers should change from the default setting to allow by exception.

3-64. DODIN operations personnel should review firewall rules to ensure security, performance, and efficiency of the firewall. The review should focus on current rules, objects redundancies, duplicate rules, and bloated rules that can cause security and management problems.

PORTS, PROTOCOLS, AND SERVICES MANAGEMENT

3-65. The DODIN operations section uses ports, protocols, and services management system to manage automated information system software on the network. This system may require unique ports, protocols, or services outside the baseline WIN-T configuration. Automated information systems and software require certification and approval under the DOD Risk Management Framework provided in DODI 8510.01.

3-66. The ports, protocols, and services management system should be able to capture and track who the user is, what the software is for, and the duration a specific port should be open. DODIN operations personnel monitor firewall logs to identify and mitigate malicious use of open ports.

NETWORK QUALITY OF SERVICE AND SPEED OF SERVICE

3-67. 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 is not acceptable. Video can become choppy and un-viewable, and voice calls can become garbled. Packets comprising an e-mail, on the other hand, eventually arrive intact with no recognizable consequence of time delays.

3-68. 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 provide 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.

Planning and Configuration

3-69. Quality of service edge device applications reside on a server between a local area network router and the colorless backbone. The network uses multiple quality of service edge devices. Configuring and implementing these devices are part of network planning. Network planners can remotely distribute and activate selected quality of service plans to all edge devices using the edge devices' web client. It also allows planners to verify which plan the edge devices are running.

Prioritizing Information

3-70. If the access control lists are empty, the network treats all traffic as default priority. If the access control list contains the entire server range, all server traffic carries the same priority. Both options are valid, but the second one can potentially have adverse effects on the network. Tailoring transmissions to a commander's priorities and polices can provide a tactical advantage. Tailoring policies improves the commanders' situational understanding and ability to control their units during unified land operations. As an example, the

S-6 may establish the quality threshold for transferring routine, non-time-sensitive information as delivery within 15 minutes, with the threshold for top priority survival information as less than 0.5 seconds.

Quality of Service Management

3-71. Determining which class of services each automated information system or service requires, based on the commander's priorities, is both complex and mission-dependent. Quality of service settings should be consistent throughout the wide-area network to work effectively. For example, an attached enabling unit may need to change their settings to match the supported brigade's quality of service plan. Figure 3-2 is a sample baseline quality of service model for a brigade with a normal distribution of mission command information systems.

	Video	Streaming	Low Latency Data	High Throughput Data	Short Message
Flash Override					JABBER, Ventrillo Chat, Transverse, CPOF Ventrillo (All Chat Applications)
Flash			DNS, Domain Controller		
Immediate			CPOF, Mid Tier, Adobe Connect		
Priority					
Routine	BVTC	UAV	Portal Page, TAIS, AFATDS, DCGS-A, CIDNE, C2PC		
Legacy					

Legend

AFATDS	Advanced Field Artillery Tactical Data System
BVTC	battlefield video teleconferencing
C2PC	Command and Control Personal Computer
CIDNE	Combined Information Data Network Exchange
CPOF	Command Post of the Future
DCGS-A	Distributed Common Ground System - Army
DNS	Domain Naming System
TAIS	Tactical Airspace Integration System
UAV	Unmanned Aerial Vehicle

Figure 3-2. Sample quality of service table

NETWORK MONITORING AND STATUS REPORTING

3-72. Network monitoring is a subordinate function to network management that more junior Soldiers can perform. Network monitoring can—

- Detect slow or failing components and links.
- Send notifications of device and network activity to a central location.
- The local node's node management function collects operational event status from managed devices and forwards the status information to the NOSC. NOSCs compile the status information for storage, analysis, and display.

3-73. When monitoring is active, the wide-area network monitoring function polls the status database continually. Some events are for information only, while others require action to mitigate the event. Either the NOSC or an individual network node may perform mitigating actions. Monitoring functions at a NOSC can become specialized. For example, one operator may exclusively monitor communications security functions while another operator performs spectrum management.

3-74. In addition to network planning, network monitoring, and node management, a NOSC provides—

- A topology generator that automatically generates a detailed network topology diagram.
- Map-based monitoring for at-the-halt and on-the-move nodes.
- Recording and playback of monitoring data.

3-75. The NOSC gathers network status and performance data through synchronous (status) and asynchronous (alert) reporting. Reporting includes—

- Synchronous reporting uses the simple network management protocol in a request-response driven polling. There are two scenarios—
  - Simple network management protocol-based commercial off the shelf software gathers and reports status.
  - The local node's operating environment messenger server performs simple network management protocol polling and forwards status updates to the NOSC's operating environment server for reporting within the network management system.
- Asynchronous reporting uses the managed device's simple network management protocol agent to alert or inform the management system of changes. There are two scenarios—
  - A simple network management protocol inform message, generated by the managed device when a specific event occurs, the managed device's agent sends a message to the management systems. The NOSC's management system must acknowledge the inform messages.
  - A simple network management protocol trap message, generated by the managed device, enables the device to report events to a NOSC management system as they occur. Trap messages occur when there is an alarm condition or configuration change. The manager does not issue an acknowledgment to a trap message.

Network Performance Reports

3-76. Network managers monitor all wide-area network links—satellite communications, line of sight, and cable—independently for bandwidth utilization. Network planners and managers use bandwidth utilization reports to inform link analysis and develop trends for identifying peak and minimum utilization periods. Results of this analysis may drive a command decision to allocate or reallocate resources to support disadvantaged locations.

3-77. For example, if a remote site has a high bandwidth requirement and is only equipped for satellite communications connectivity, users may experience problems with network congestion and latency. Moving a high capacity line of sight terminal to support the remote site increases the available throughput, reduces costly satellite communications bandwidth requirements, decreases latency, and provides redundant network transport.

Transmission Reports

3-78. Transmission reports identify degradation in transmission systems or link quality before they create link outages. A transmission report includes signal strength, energy per bit to noise power spectral noise density ratio (Eb/N0 the ratio of Energy per Bit (Eb) to the Spectral Noise), bit error rate, error count, and alarms over a specified period. Transmission reports should include all transmission systems—STT, high capacity line of sight, and Highband Networking Radio. Figure 3-3 on page 3-14 shows a sample high capacity line of sight outage report.

HCLOS OUTAGE

TRAINED DATE	TRAINED INITIALS	VERIFIED DATE	VERIFIED INITIALS	TASK
				1. Identify link with packet loss.
				- through SNMPc
				- ping test
				2. Loops
				- local patch panel loopback
				- local flex-mux loopback
				- local HVA loopback
				- local cable loopback
				- RF loopback
				- distant end flex-mux loopback
				3. Tests
				- data cable TQM test
				- VSWR test
				- radio loop test
				- input loop test
				- spectrum scan test

Verified by: _____ Soldier: _____

LEGEND:

HCLOS	high-capacity line of sight
HVA	high voltage amplifier
mux	multiplexer
RF	radio frequency
TQM	technical quality measures
VSWR	vertical standing wave ratio

Figure 3-3. Sample high capacity line of sight outage report

3-79. Figure 3-4 shows a sample satellite communications transmission report.

8-HOUR SATCOM REPORT				
		0000	0800	1600
ASSEMBLAGE				
LINK TO				
RSL				
Eb/N0				
TPO				
WEATHER				
TRACKING				
INITIALS				

LEGEND:

Eb/N0	energy per bit to spectral noise density ratio
RSL	receive signal level
SATCOM	satellite communications
TPO	total power out

Figure 3-4. Sample satellite communications transmission report

Communications Status Report

3-80. The communications status report is a daily report of all network node status. This provides an accurate view of the network during shift change, and informs the G-6 (S-6) of the network's condition. The communications status report should include all battalion nodes and attached enablers. The communications status report includes planned network changes and service interruptions.

SHIFT CHANGES

3-81. Structured shift changes help with effective information exchange between the incoming and outgoing shifts. Operators record shift change information in the team's master station log for historical reference. At a minimum, the shift change briefing should capture—

- Significant events over the previous shift—including outages and equipment failures.
- Planned events for the next shift.
- Pertinent administrative information.

DIGITAL BATTLE DRILLS

3-82. Battle drills provide operators and DODIN operations teams structured, pre-planned responses to network, communications security, cybersecurity, power outage or server-related events. Established standards are easy to enforce and improve expectation management inside the command. All echelons should formulate and actively rehearse battle drills for a variety of anticipated events to ensure timely and appropriate responses. Unit leaders should provide attached enabling elements copies of the unit's battle drills and actively include enablers in rehearsals. Figure 3-5 on page 3-16 shows a sample battle drill for malicious software found on the network.

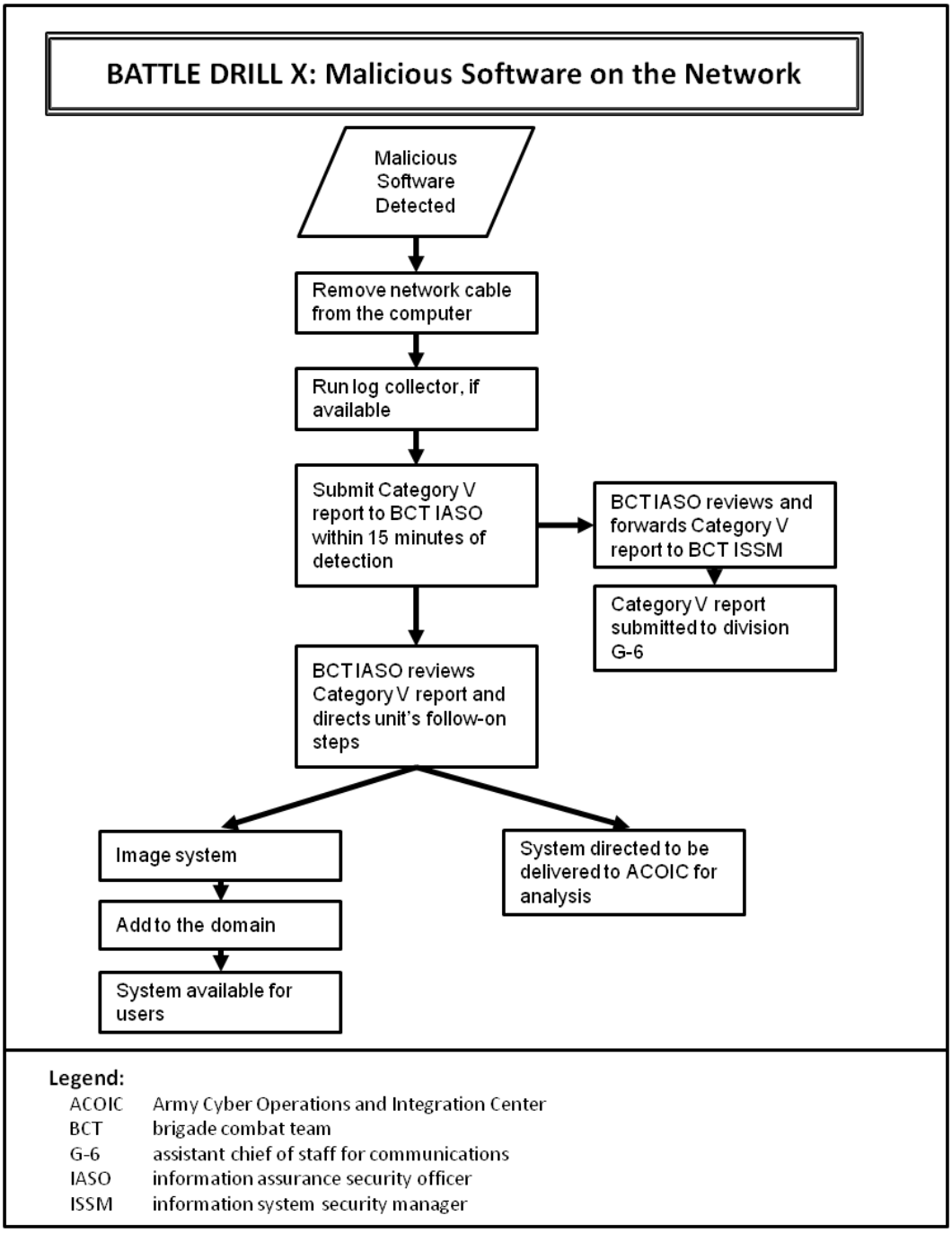

Figure 3-5. Sample battle drill

UNCLASSIFIED COMMUNICATIONS BLACKOUT

3-83. Units require a plan to block unofficial communications between the time a casualty occurs and the official notification of the next of kin. This prevents unofficial disclosure by well-meaning individuals in the unit. The unit may also implement an unclassified communications blackout (NIPRNET blackout) if a Soldier is in duty status—whereabouts unknown.

3-84. The DODIN operations section may implement a NIPRNET blackout using an access control list to block IP traffic, allowing by exception according to command guidance. In order to be effective, the unofficial communications blackout plan should also address the use of personal communications devices, such as cellular phones and personal computers using commercial internet service.

CONFIGURATION MANAGEMENT

3-85. DODIN operations personnel establish baseline configurations of all network devices. Device configurations may evolve over time as missions change. DODIN operations personnel should avoid restoring WIN-T to its pre-validation exercise configuration. Network managers should restore the system to the established baseline before each new mission to remove any previous mission-specific configuration.

3-86. The Defense Information Systems Agency's security technical implementation guides provide DOD-wide configuration standards for cybersecurity and cybersecurity-enabled devices and systems. Default WIN-T configurations may not meet security technical implementation guide requirements. Units should periodically download the current applicable security technical implementation guides and ensure their configurations meet these requirements to mitigate vulnerabilities. The security technical implementation guide requirements are available on the DOD Cyber Exchange Website.

3-87. The brigade NOSC maintains the configuration for the entire brigade combat team network, including attached support elements. Brigade DODIN operations personnel prepare the configurations necessary to integrate support elements into the network and allow themselves to access, monitor, and manage these systems. The brigade NOSC does not need permission to make configuration changes to support elements. The attached node maintains a backup copy of their pre-mission configuration so they can easily return to baseline upon mission completion.

3-88. Scheduled, periodic backups of all network devices should be part of the operator and DODIN operations section battle rhythms. Operators should also create a backup after any configuration change. Network managers should compare and contrast backup configurations periodically to identify unplanned network changes. DODIN operations personnel should archive backup configurations to create historical mission records as reference material for future missions.

3-89. Network managers should post procedures to restore configurations at each network node. This facilitates restoring network connectivity after a device failure. Managers should integrate restoration procedures into the section's cross-training plan. Refer to ATP 6-02.71 for more information about configuration management.

This page intentionally left blank.

Chapter 4
Employment and Training

The deployed network connects tactical forces at all levels with the operational force and sustaining base. The network is scalable to support command posts ranging from battalion command vehicles and small command posts to larger and more complex command posts at the battalion, brigade, division, and corps. Section I discusses command post support and command post survivability. Section II discusses employment of WIN-T communications systems to provide upper tier tactical internet support to command posts at echelons corps through battalion and in support brigades. Section III discusses individual and collective training for signal systems.

SECTION I – COMMAND POST SUPPORT

4-1. Command posts contain vital systems for the command and control warfighting function. They also provide military leaders with the capability to make timely decisions, communicate those decisions to subordinate units, and monitor the execution of these decisions.

COMMAND POST SURVIVABILITY

4-2. Command post survivability is vital to mission success. Depending on the threat, command posts need to remain small and highly mobile, especially at lower echelons. Command posts are easy for enemies to locate and target when concentrated.

4-3. Methods to enhance command post survivability include—dispersion, size, electronic signature, redundancy, mobility, camouflage, concealment, deception, use of decoys, continuity of operations, and PACE planning. Additional measures include cover or shielding by terrain features or urban structures. The considerations in this section apply to command posts at all echelons. Refer to ATP 3-37.34 for more information on command post survivability.

DISPERSION

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

FREQUENT DISPLACEMENT

4-5. Command posts need to relocate frequently during large-scale combat operations against a peer threat. Maintaining continuity during displacement of a command post or catastrophic loss requires designating alternate command posts and passing control between command posts (FM 3-0). Command post displacement requires advance coordination and battle handover so at least one command post is always available to control the fight.

MOBILITY

4-6. Command post mobility is important, especially at lower echelons during combat operations. Lower-echelon command posts and those employed forward in the combat zone may need to move quickly and often. Small size and careful planning enable rapid and effective command post displacement.

SIZE

4-7. The size of a command post affects its mobility and survivability. Large command posts may increase capacity and enhance face-to-face coordination and collaboration, but their size makes them vulnerable to multiple means of acquisition and attack. Smaller command posts are easier to protect, but may not have the capacity to control operations effectively.

REDUNDANCY

4-8. Reducing command post size reduces detectability and enhances mobility. However, some personnel and equipment redundancy is necessary to maintain continuous operations. During periods of high operational tempo, personnel and equipment are subject to combat loss and failure due to stress. The right amount of redundancy allows command posts to continue to operate effectively.

SIGNATURES

4-9. 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.

Electromagnetic

4-10. A large number of antennas, their electronic 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 at from the back and sides of directional antennas.

4-11. When evaluating electromagnetic signatures emitted by command posts, planners should consider concentrations of vehicles, wear and track marks due to heavy traffic, and air traffic. Parking vehicles and aircraft away from command posts mitigates the concentrated electromagnetic signature.

4-12. Command posts conduct electronic masking using electromagnetic decoys to protect the locations of critical nodes. *Electronic 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 electronic warfare support measures/signals intelligence without significantly degrading the operation of friendly systems (JP 3-13.1). Electromagnetic decoys used for masking radiate at higher energy levels than normal communications to hide real transmission from enemy electronic warfare support and signals intelligence capabilities. Refer to ATP 3-12.3 for more information about electronic masking.

Visual

4-13. Command posts require excellent camouflage and concealment to survive on the battlefield. Camouflage and concealment improve operations security and increase survivability by minimizing the observable size of command posts. Command post camouflage and concealment require reconnaissance, planning, discipline, security, and maintenance. Reconnaissance and heightened security patrols enhance camouflage and concealment efforts by denying access to vantage points from which an enemy can observe a command post.

4-14. Defensive positions often create scarred earth signatures and detectable patterns due to earth excavation. While defensive position are critical to command post survivability, units should mitigate the visual signatures of defensive positions by taking advantage of available natural cover and concealment. Planners should consider the following regarding camouflage and concealment for command posts—

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

Radar

4-15. Radio frequency reflective camouflage netting can help reduce the radar signature of command posts. Barbed wire exhibits a measurable radar cross section at radar frequencies. Emplacing barbed wire and concertina wire to follow natural terrain features, when possible, reduces their radar signature.

Infrared (Thermal)

4-16. Power generators and other heat sources produce thermal signatures that enemy surveillance and target acquisition sensors can detect. Emplacing heat-producing equipment and other thermal sources in defilade positions, within structures or under natural cover mitigates their infrared signature. Heat diffusers that disperse and vent vehicle exhaust away from the threat direction, are an expedient means of thermal signature reduction.

Noise

4-17. Noise discipline contributes to command post survivability. The power generation equipment associated with signal equipment can generate significant noise. During site selection, signal leaders should consider measures to mask and diffuse the noise from electrical generators.

SECTION II – EMPLOYMENT BY ECHELON

4-18. WIN-T increment 2 provides network transport for command and control information and applications, both at-the-halt and on-the-move. These capabilities meet the unique requirements of divisions and brigade combat teams. Increment 1b systems provide the same services as increment 2 systems at-the-halt only. Each unit has an equipment complement tailored to their echelon and unit type. These configurations ensure the unit's organic communications equipment supports its command posts and command and control on-the-move requirements

CORPS

4-19. The corps is the operational headquarters for decisive land combat and includes enhanced capabilities for unified land operations. The corps defines the fight, ensures coherency, conducts operational maneuver, and serves as the bridge to translate strategic guidance into tactical tasks. The corps staff divides into two command posts. This expands the commander's ability to exercise command and control, and makes the command and control system more survivable. A deployed corps headquarters remains relatively static, so it does not require WIN-T increment 2's on-the-move capabilities. The corps' organic increment 1b equipment provides its WIN-T support, operated by elements of the corps signal company.

MAIN COMMAND POST

4-20. The corps main command post synchronizes the conduct of current operations and allocates available resources. Under the general supervision of the corps chief of staff, it also oversees the conduct of future planning, analysis for current and future operations, sustainment coordination, and other staff functions.

TACTICAL COMMAND POST

4-21. The corps tactical command post normally functions as an additional current operations cell colocated with the main command post. This command post can also operate independently to control corps operations for a limited time and can form the nucleus of an early-entry command post. Table 4-1 on page 4-4, shows the allocation of WIN-T increment 1b systems in the corps.

Table 4-1. Increment 1b allocation in the corps

Command Post	*Joint Network Node*	*Satellite Transportable Terminal*	*Secure Mobile Anti-Jam Reliable Tactical Terminal*	*High capacity line of sight*	*Modular Communications Node-Advanced Enclave*
Main	1	1	1	—	2
Tactical	2	2	2	2	2

DIVISION

4-22. Division headquarters support their main, tactical, and support area command posts with organic WIN-T assets. This support varies by capability set—increment 2 or increment 1b.

INCREMENT 2

4-23. WIN-T increment 2 systems provide access to the DODIN-A for the division headquarters to access to mission-command-enabling systems and DISN services in the upper tier tactical internet. These systems provide joint and Army interoperability so warfighters can access information services using line of sight and military or commercial satellite communications transport.

4-24. Commanders of increment 2-enabled units can dynamically tailor their assigned forces and network capabilities to meet their requirements across the range of military operations. WIN-T allows division commanders to tailor their network to mission, task, and purpose. Increment 2 allows the division headquarters to receive and share information both at-the-halt and on-the-move. This allows warfighters to visualize and selectively control their area of operations while planning and conducting operations.

4-25. Soldiers from the signal portion of the division signal, intelligence, and sustainment company install, operate, and maintain the division's WIN-T assets. The division's organic WIN-T system allocations support the main command post, the tactical command post, and the mobile command group.

Main Command Post

4-26. The main command post is the division's primary command post—the heart of the division's operation. The main command post is usually located out of the range of the enemy's medium artillery. Though the division main command post is mobile, it operates mainly at-the-halt.

Tactical Command Post

4-27. When fully active, the division tactical command post controls the close operation. The division tactical command post is a small, highly mobile, and survivable command post normally located close to the forward brigades. The division tactical command post operates at-the-halt or on-the-move.

Support Area Command Post

4-28. The division support area command post has no organic communications system allocations. The division G-6 and signal company support communications and network requirements using organic equipment and personnel authorizations or request support from external sources. Requests for communications support for the support area command post follow the request for forces process in FM 6-02.

Mobile Command Group

4-29. The mobile command group serves as the commander's mobile command post. It consists of ground and air components equipped with information systems. These vehicles and aircraft allow commanders to move to critical locations to personally assess a situation, make decisions, and influence operations. The mobile command group's information systems and small staff allow commanders to do this while retaining communications with the entire force (FM 3-0). See table 4-2 on page 4-5, for increment 2 system allocations in the division headquarters.

Table 4-2. Increment 2 allocations in the division headquarters

	Command post type			
Node type	***Main***	***Tactical***	***Support area***	***Mobile Command Group***
Tactical hub node	1	—	—	—
Tactical Communications Node	1	2	—	—
Satellite Transportable Terminal	1	2	—	—
Tactical Relay-Tower	—	1	—	—
SMART-T	1	2	—	—
NOSC	—	2	—	—
Point of Presence	2	1	—	1
MCN-AE	2	2	—	—
Commercial Coalition Equipment				—
Legend:				
MCN-AE	Modular Communications Node-Advanced Enclave			
NOSC	network operations and security center			
SMART-T	Secure Mobile Anti-Jam Reliable Tactical Terminal			

INCREMENT 1B

4-30. In increment 1b-equipped divisions, G-6 and signal, intelligence and sustainment company support the command post using assigned tactical hub node, Joint Network Nodes, and Command post nodes. These organic assets provide communications support at the main, tactical, and support area command posts.

Main Command Post

4-31. The main command post usually locates out of the range of the enemy's medium artillery. The division main command post operates at-the-halt, but must displace frequently during large-scale combat operations.

Tactical Command Post

4-32. The division tactical command post is a small, highly mobile, and survivable command post normally located close to the forward brigades. The tactical command post controls the division's operations during displacement of the main command post.

Support Area Command Post

4-33. The division support area command post has no organic communications system allocations. The division G-6 and signal company support communications and network requirements using organic

equipment and personnel authorizations or request support from external sources. Requests for communications support for the support area command post follow the request for forces process in FM 6-02. Table 4-3 shows the allocation of WIN-T increment 1b systems in the Reserve Component division headquarters.

Table 4-3. Increment 1b allocation in the Reserve Component division

Command Post	*JNN*	*STT*	*SMART-T*	*HCLOS*	*MCN-AE*	*THN*
Main	1	1	1	—	2	1
Tactical	2	2	2	2	2	—
Support Area	—	—	—	—	—	—
Legend:						
HCLOS	high capacity line of sight					
JNN	Joint Network Node					
MCN-AE	Modular Communications Node-Enhanced Enclave					
SMART-T	Secure Mobile Anti-Jam Reliable Tactical Terminal					
STT	Satellite Transportable Terminal					
THN	tactical hub node					

BRIGADE COMBAT TEAM

4-34. Brigade combat teams usually conduct operations from two command posts, the brigade main command post, and the brigade tactical command post. Brigade signal company Soldiers install, operate, and maintain WIN-T equipment to support the main and tactical command posts.

INCREMENT 2

4-35. Increment 2 systems allow the brigade combat team S-6 to allocate communications capacity according to the commander's priorities while controlling, monitoring, and maintaining the network. With transport convergence, increment 2 provides top secret sensitive compartmented information network transport for the brigade command posts.

Main Command Post

4-36. The main command post is the unit's principal command post. It includes representatives of all staff sections and a full suite of information systems to plan, prepare, execute, and assess operations. The main command post is larger, has more staffing, and is less mobile than the tactical command post. The main command post operates mainly at-the-halt, though it can operate with reduced capacity on-the-move.

Tactical Command Post

4-37. The tactical command post is fully mobile and usually is located near the decisive point of the operation. The tactical command post operates on-the-move or at-the-halt. See table 4-4 on page 4-7 for increment 2 system allocations in the brigade combat team.

Table 4-4. Increment 2 allocations in the brigade combat team headquarters

Node type	*Main command post*	*Tactical command post*
Tactical Communications Node	X	X
Point of presence	X	X
Soldier Network Extension		X
Satellite Transportable Terminal	X	X
Tactical Relay-Tower	X	
SMART-T	X	X
HCLOS	X	
NOSC	X	
MCN-AE	X	X

Legend:

HCLOS	high capacity line of sight
MCN-AE	modular communications node-enhanced enclave
NOSC	network operations and security center
SMART-T	Secure Mobile Anti-Jam Reliable Tactical Terminal

Maneuver and Support Battalions (Brigade Combat Team)

4-38. Maneuver battalions receive communications support from organic Soldiers and equipment. Soldiers in the battalion S-6 install, operate, and maintain the battalion's organic WIN-T systems. The battalion S-6 identifies communications requirements. The brigade NOSC performs DODIN operations for the battalion's upper tier tactical internet. Refer to ATP 6-02.53 for more information about DODIN operations in the lower tier tactical internet. Active Component maneuver and support battalion's WIN-T increment 2 allocations are—

- TCN.
- Satellite Transportable Terminal.
- Point of Presence.
- Soldier Network Extension.

INCREMENT 1B

4-39. WIN-T increment 1b systems allow the S-6 to allocate communications capacity according to the commander's priorities while controlling, monitoring, and maintaining the network. With transport convergence, WIN-T provides network transport for sensitive compartmented information networks for the brigade command posts. The Modular Communications Node-Advanced Enclave provides user connections to sensitive compartmented information networks.

Main Command Post

4-40. The main command post is the unit's principal command post. It includes representatives of all staff sections and a full suite of information systems to plan, prepare, execute, and assess operations. The main

command post is larger, has more staffing, and is less mobile than the tactical command post. The main command post usually locates farther from the decisive point, outside the range of enemy artillery.

Tactical Command Post

4-41. The tactical command post is fully mobile and usually is located near the decisive point of the operation. The tactical command post controls the main operation when the main command post displaces. See table 4-5 for increment 1b system allocations in Reserve Component and armored brigade combat teams.

Table 4-5. Increment 1b allocations in the Reserve Component and armored brigade combat team

Command Post	*JNN*	*STT*	*HCLOS*	*MCN-AE*
Main	1	1	1	1
Tactical	1	1	1	1
Legend				
HCLOS	high capacity line of sight			
JNN	Joint Network Node			
MCN-AE	Modular Communications Node-Advanced Enclave			
STT	Satellite Transportable Terminal			

Maneuver and Support Battalions

4-42. Maneuver and support battalions receive communications support using Soldiers and equipment from the brigade signal company. The battalion S-6 identifies communications requirements for the command post and installs, operates, and maintains automated information systems, telephone equipment, and the command post local area network.

4-43. The brigade NOSC performs DODIN operations for the battalion's upper tier tactical internet. Refer to ATP 6-02.53 for more information about DODIN operations in the lower tier tactical internet. Reserve Component maneuver and support battalion's WIN-T support uses—

- Joint Network Node.
- Satellite Transportable Terminal.

SUPPORT BRIGADES

4-44. Support brigades' areas of operation are less dynamic than those of divisions and brigade combat teams. For this reason, they do not require the command and control on-the-move capabilities of increment 2, but they must still be capable of displacing command posts on short notice. Multifunctional support brigades use organic increment 1b equipment to provide command and control-enabling applications and DISN services. Functional support brigades receive signal support from elements of the theater tactical signal brigade.

MULTIFUNCTIONAL SUPPORT BRIGADE

4-45. Combat aviation, field artillery, sustainment, and maneuver enhancement brigades receive their reachback, command and control-enabling applications, and DISN services using organic WIN-T increment 1b systems.

Brigade Command Post

4-46. Brigade signal company Soldiers install, operate, and maintain these systems to meet the commander's requirements. The brigade S-6 identifies these requirements. Unlike the division and brigade combat team, support brigades maintain one command post.

Support Battalion

4-47. The support battalion receives its WIN-T support using Soldiers and equipment from the brigade signal company. The battalion S-6 identifies communications requirements. The brigade performs DODIN operations for the support battalion's WIN-T equipment. The battalion S-6 provides its own automated information systems and manages the battalion's local area network. See table 4-6 for the battalion's WIN-T system allocations in multifunctional support brigades and support battalions.

Table 4-6. Increment 1b allocation in multifunctional support brigades

Command Post	*Joint Network Node*	*Satellite Transportable Terminal*	*Command Post Node*	*Secure Mobile Anti-Jam Reliable Tactical Terminal*	*High capacity line of sight*
Combat aviation brigade	1	1	5	1	3
Field artillery brigade	1	1	4	1	3
Sustainment brigade	1	1	2	—	3
Maneuver enhancement brigade	1	1	3	—	3
Support battalion	—	1	1	—	—

EXPEDITIONARY SIGNAL BATTALION

4-48. Certain units do not have organic signal assets. However, they still need the same services and applications as maneuver units when deployed. The pooled theater assets of an expeditionary signal battalion are available to provide them WIN-T support. The expeditionary signal battalions provide modular support. They employ Joint Network Node and Command Post Node teams as needed to meet specifically tailored support requirements. Refer to FM 6-02 and Army doctrine for theater signal support for more information about obtaining communications support from an expeditionary signal battalion.

4-49. The expeditionary signal battalion provides nodal and extension communications for deployed Army and joint units. Supported headquarters may include combatant commands, Army Service component commands, joint task force headquarters, or joint force land component commands with no organic communications assets or insufficient assets.

4-50. The on-the-move communications capabilities of WIN-T increment 2 meet the unique needs of brigade combat teams and divisions by design. Since support units do not require the same capability, the expeditionary signal battalion's WIN-T systems are increment 1b. They provide network centric waveform satellite communications to interface with the regional hub node and increment 2 equipped units, but not the increment 2 on-the-move capabilities.

4-51. The expeditionary signal battalion provides—

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

Expeditionary Signal Company

4-52. The expeditionary signal company provides home station-quality DISN and command and control-enabling services to small and medium command posts. This includes line of sight and beyond line of sight network transport, network management, and cable and wire systems. The expeditionary company provides tailored communications packages consisting of one or more of the equipment systems shown in allocation table 4-7.

Table 4-7. Increment 1b allocations in the expeditionary signal company

	Team type			
Equipment type	***TACSAT***	***Medium network***	***Small network***	***LOS v3***
Phoenix	2	—	—	—
JNN	—	2	—	—
STT	—	2	10	—
CPN	—	—	10	—
LAN manager	—	—	10	—
HCLOS v1	—	—	10	—
HCLOS v3	—	—	—	4

Legend:

CPN	Command Post Node
HCLOS	high capacity line of sight
JNN	Joint Network Node
LAN	local area network
STT	Satellite Transportable Terminal
TACSAT	tactical satellite

Joint/Area Signal Company

4-53. The joint/area signal company provides home station-quality DISN and command and control-enabling services to large and medium command posts and command post clusters. This includes line of sight and beyond line of sight network transport, network management, and cable and wire systems. The joint/area signal company provides tailored communications packages consisting of one or more of the equipment systems shown in allocation table 4-8 on page 4-11.

Table 4-8. Increment 1b allocations in the joint/area signal company

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

Legend:

CCE	Commercial Coalition Equipment
HCLOS	high capacity line of sight
LAN	local area network
LOS	line of sight
SMART-T	Secure Mobile Anti-Jam Reliable Tactical Terminal
TACSAT	tactical satellite
TROPO	tropospheric scatter

SECTION III – TRAINING

INDIVIDUAL TRAINING AND CERTIFICATION

4-54. Soldiers are assigned to meet units' specific military occupational specialty and grade requirements. Units establish unit-specific supervised on-the-job training plans and operator certification standards to ensure their Soldiers are proficient in the required critical tasks. WIN-T refresher training is available online at the Project Manager Tactical Network Information and Support Exchange Website.

CROSS-TRAINING

4-55. Developing and implementing a cross-training plan ensures Soldiers can perform basic tasks on most WIN-T equipment, regardless of their military occupational specialty. An effective cross-training plan enables signal teams to establish, sustain, and displace WIN-T systems more quickly and efficiently, and to a higher standard. Cross-training WIN-T operators to perform basic tasks outside of their military occupational specialties develops signal Soldiers with greater depth and experience, and increased confidence. This is especially important during times of reduced manning and during 24-hour operations.

4-56. Each member of a team should be familiar with the basic tasks every member of that team. Leaders cannot be expect them to be experts on areas outside their military operational specialties, but Soldiers should be able to help install systems, identify when the systems are operating correctly, and get assistance when something goes wrong.

4-57. The cross-training plan should include the most commonly performed, basic operator tasks. This reduces reliance on key team members. The plan should be flexible enough to adapt to changing mission and manning requirements. Some examples of cross-training for WIN-T operators are—

- Training Joint Network Node team operators to perform DODIN operations in the brigade NOSC. This provides flexibility in manning the NOSC and gives the Joint Network Node team operators experience in more advanced network troubleshooting and management.
- Training all operators to add a VoIP phone to the Unified Communications Manager, and change display names and caller identification information.
- Training all operators on a Command Post Node team to verify the Satellite Transportable Terminal is tracking the satellite, and the satellite communications modem is in synchronization with the network controller.
- Training all WIN-T operators to check signal strength and errors on high capacity line of sight systems.

4-58. Crew drills are an effective mechanism to validate and sustain team training. Teams should train and conduct crew drills according to the unit's combined arms training strategy or standard operating procedure. The unit should implement team and crew certification standards to support the unit's mission, and incorporate these standards into their operational planning considerations.

UNIT TRAINING

4-59. Units frequently only make time for WIN-T operator training when the unit goes to the field. This is not an acceptable practice, since network disruptions interfere with the larger exercise. Proper command emphasis can ensure operators and teams are proficient on their systems before field exercises. This training may take place in the unit's motor pool or a garrison training area, with or without the need for satellite time.

4-60. Units training at their home station or preparing for deployment to support significant training events utilize either installation as a docking station or their tactical hub node for DISN access. Whenever possible, they should limit regional hub node access to significant training events, such as combat training center rotations and real world missions, unless bridging increment 1b and increment 2 networks.

COLLECTIVE TRAINING TECHNIQUES

4-61. Collective training follows an integrated approach of live, virtual, and constructive training at home station, combat training center rotations, and during deployments to build confident, cohesive units able to adapt to their environment and defeat the enemy. Demanding and repetitive training builds Soldiers' confidence in their weapons and equipment, their ability to fight and overcome challenges, their leaders, and their teams.

REALISTIC TRAINING ENVIRONMENT

4-62. The training environment should duplicate the anticipated operational environment and threat. Teams train under conditions that emphasize change, uncertainty, degraded friendly capabilities, capable enemies, and austere conditions. Realistic training prepares Soldiers to perform under combat conditions by including unexpected tasks and battle drills.

4-63. Commanders should incorporate a realistic threat environment into training exercises, so teams learn to recognize indications of cyberspace attacks and jamming. Understanding network vulnerabilities is critical. The training environment should include likely adversary tactics, techniques, and procedures. Units must train to identify key terrain in cyberspace relative to their commander's priorities to enable a focused defense. Establishing a properly configured, monitored, and secured network during training events prepares operators to detect malicious and unauthorized activity and enables command and control and the other warfighting functions.

4-64. Integrating training with a realistic threat able to attack networks into unit training at home station and combat training centers prepares units for real-world missions. It also prepares units to understand the threat and indicators of a contested environment. Realistic training also demonstrates the consequences of not following security procedures.

4-65. A realistic training environment provides operators practice securing the DODIN-A against active threat and allows units to integrate actions and effects in support of maneuver commanders. Training signal forces to secure the network against an active threat is critical to mission success. Realistic and combat-focused training requires specialized technical training, instrumentation, and ranges at home station and combat training centers.

DIGITAL BATTLE DRILLS

4-66. Unit standard operating procedures should establish digital battle drills for a range of likely emergencies. Digital battle drills provide operators structured, pre-planned responses to network, communications security, cybersecurity, or server-related events or power outages. Realistic training and repetition ensure operators can perform conditioned responses reflexively under combat or other emergency conditions.

COMBINED ARMS TRAINING STRATEGY

4-67. The signal company's training calendar should include events from the combined arms training strategy. These training events progressively build from team level through multi-echelon exercises supporting the parent unit. The combined arms training strategy begins with team tasks to develop crew proficiency installing and operating assigned systems. Successive platoon- and company-level training exercises ensure the teams can integrate network systems into the DODIN-A. Training signal teams to proficiency through the combined arms training strategy ensures Soldiers remain proficient in their individual military occupational specialty skills and can integrate the network to support operations.

This page intentionally left blank.

Appendix A

Operations in a Contested Environment

This appendix addresses the means to recognize and overcome threat activities affecting signal support in a contested environment. It includes an overview of peer threat tactics, techniques, and procedures and methods to counter threat electronic warfare and cyberspace attacks.

THREAT TACTICS, TECHNIQUES, AND PROCEDURES

A-1. A peer threat's information warfare activities will integrate electronic attack, military deception, lethal fires, perception management, information attack, and computer warfare to deny U.S. and allied forces access to the electromagnetic spectrum in a contested environment.

A-2. Understanding threat capabilities in the electromagnetic spectrum is key to sound signal support plans. Enemy attacks on friendly command nodes may combine electronic attacks, other information warfare effects, and lethal fires to deny friendly forces the use of spectrum-dependent systems. To accomplish this goal, threat forces gather technical and combat information about their enemies. As enemy forces locate and identify friendly units, enemy information warfare elements establish priorities to—

- Jam communications assets.
- Deceptively enter radio networks.
- Interfere with the normal flow of U.S. and allies' communications.

MEASURES TO PREVENT THREAT EFFECTS

A-3. Understanding threat capabilities is critical to hardening the deployed network against enemy electronic warfare and signals intelligence. If an enemy cannot detect command posts and communications sites, it cannot target the sites with electronic attack or lethal fires.

LIMITING ELECTROMAGNETIC SIGNATURE

A-4. To protect against a peer threat's ability to locate and target radio signals, the G-6 (S-6) must plan signal support in a way that limits the electromagnetic signature of the command post. Measures to reduce the electromagnetic signature of command posts and communications sites include—

- Careful siting of radio equipment.
- Employment of directional antennas.
- Operations using lowest power required.
- Limiting radio transmissions.
- Using a random schedule.

A-5. Electronic protection techniques can also help mask the electromagnetic signature. The cyber electronic warfare officer can assist the G-6 (S-6) in planning electronic protection measures to reduce the command post signature.

Terrain Masking

A-6. Terrain masking can effectively block radio signals from reaching enemy direction finding capabilities. Positioning communications systems with large terrain features or manmade structures

between the communications system and the forward line of own troops effectively blocks an enemy from detecting the signal.

Camouflage Net Masking

A-7. Radar reflective camouflage netting is an effective means of blocking stray electromagnetic radiation from directional antennas. Camouflage netting placed to the sides and back of a line of sight or satellite communications antenna ensures only the main beam of the antenna radiates. Since the main beam is directional, it is much harder for the enemy to detect; the enemy would need to be directly in the transmission path.

Line of Sight

A-8. High-throughput line of sight radios can carry high bandwidth data over distances up to 40 kilometers. Planners should engineer links to minimize chances of detection, targeting, and jamming. If the line of sight path is parallel to the forward line of troops, an enemy is less likely to detect the signal, and enemy jammers cannot reach the antenna with a strong enough signal to jam the radio.

Satellite Site Selection and Radio Frequency Interference

A-9. WIN-T satellite communications systems suffer from natural and manmade interference. Natural sources of interference include solar activity, dense vegetation, thick cloud cover, heavy precipitation, and sandstorms. Manmade sources of interference include vehicles, buildings and other structures that obstruct the line of sight path to the satellite, jamming, and radio frequency interference.

A-10. Commanders and staffs need to identify and minimize the command post footprint and electromagnetic signature. Planners and operators should identify physical surroundings to minimize interference and mask the electromagnetic signatures of deployed communications systems. Refer to ATP 6-02.70 for more information on radio frequency interference.

A-11. Signal elements operating from locations without masking terrain features or structures can use power settings and radio frequency management techniques, to control interference and detection. When establishing satellite communications links, the equipment operator should communicate with satellite network controllers to determine the minimum required power level. The possibility of interference, detection, and signal jamming increases as output power increases. Refer to ATP 6-02.53 and Army doctrine on electronic warfare for more information on masking and power settings. Refer to ATP 6-02.54 for more information about satellite communications.

REMOTE ANTENNAS

A-12. Large command posts and high-throughput communications systems emit a significant amount of electromagnetic energy. While planners and operators can mask some of this energy with directional antennas, site selection, terrain masking techniques, but some energy remains. Because command and control capabilities are a priority target for peer threats, anything near the communications system is at risk of destruction from lethal fires.

A-13. Commanders and signal planners should consider locating major communications assemblages as far from the supported command post as practical. Selecting a site with terrain features, manmade structures, or distance between communications systems and command posts protects the command post from lethal fires. Commanders and planners must consider the additional physical security and site defense requirements for a remote site during planning.

FREQUENT COMMAND POST DISLOCATION

A-14. Despite efforts to reduce and mask the electromagnetic signature of a command post, a peer threat may eventually locate it. Moving a command post frequently reduces its chance of destruction. This is especially important when operating within the range of enemy artillery. Peer threats are able to direct a high volume of lethal fires to destroy an area target quickly.

A-15. Maintaining continuity during displacement of a command post or catastrophic loss requires designating alternate command posts and passing control between command posts (FM 3-0). During training exercises, units must practice frequent command post dislocation and handoff between the main and tactical command posts.

SATELLITE SITE SELECTION AND RADIO FREQUENCY INTERFERENCE

A-16. The WIN-T satellite communications systems suffer from natural and manmade interference. Natural sources of interference include solar activity, dense vegetation, thick cloud cover, heavy precipitation, and sandstorms. Manmade sources of interference include vehicles, buildings, and other structures that obstruct the line of sight path to the satellite, jamming, and radio frequency interference.

A-17. Commanders and staffs need to identify and minimize the command post footprint and electromagnetic signature. Planners and operators should identify physical surroundings to minimize interference and mask the electromagnetic signatures of deployed communications systems. Refer to ATP 6-02.70 for more information on radio frequency interference.

A-18. Signal elements operating from locations without masking terrain features or structures can use power settings and radio frequency management techniques, to control interference and detection. When establishing satellite communications links, the equipment operator should communicate with satellite network controllers to determine the minimum required power level. Using a higher power signal than needed for communications increases the likelihood an enemy detection and targeting of the communications capability. Refer to ATP 6-02.53 and ATP 3-12.3 for more information on masking and power settings. Refer to ATP 6-02.54 for more information about satellite communications.

RECOGNIZING AND RESPONDING TO THREAT EFFECTS

A-19. Because peer threats consider friendly command and control capabilities to be high priority targets, they have developed capabilities to deny their enemies the effective use of the electromagnetic spectrum for communications. Signal Soldiers and leaders must learn to identify and respond to threat effects in cyberspace and the electromagnetic spectrum.

ELECTROMAGNETIC JAMMING

A-20. *Electromagnetic jamming* is deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy's combat capability (JP 3-13.1). Jamming is an effective way for the enemy to disrupt friendly communications. An enemy only needs a transmitter tuned to a U.S. frequency with enough power to overpower friendly signals can effectively jam U.S. systems.

A-21. Jammers operate against receivers, not transmitters. The two modes of jamming are spot and barrage jamming. Spot jamming concentrates power on one channel or frequency. Barrage jamming is power spread over several frequencies or channels at the same time. It is important to recognize jamming, but it can be difficult to detect. Refer to ATP 3-12.3 and ATP 6-02.53 for more information about electromagnetic jamming.

Communications Jamming

A-22. Radio operators must learn to recognize and react to electromagnetic jamming. This is not always an easy task, since electromagnetic interference can be either internal or external. Other sources having nothing to do with enemy jamming may cause electromagnetic interference. Unintentional electromagnetic interference may be caused by one or more of—

- Other radios (friendly and enemy).
- Other electronic, electrical, or electromechanical equipment.
- Atmospheric conditions.
- Equipment malfunction.

A-23. Radio operators must train to differentiate internal and external interference quickly. Refer to ATP 6-02.53 for more information about isolating and eliminating internal sources of interference.

A-24. Electromagnetic jamming most commonly affects single-channel radio systems. These radios include HF, VHF, and UHF radios. Jamming effects may be obvious or subtle. Obvious jamming is normally simple to detect. When experiencing jamming, it is more important to recognize and overcome the incident than to identify it formally.

A-25. Subtle jamming is less obvious because subtle jamming signals produce no sound from the receivers. Although everything may appear normal to the radio operator, the receiver cannot receive an incoming friendly signal. Often, users assume their radios are malfunctioning, instead of recognizing subtle jamming. Table A-1 on page A-5 lists some common jamming signals.

Table A-1. Common jamming signals

Signal	*Description*
Random Noise	Synthetic radio noise. It is indiscriminate in amplitude and frequency. It is similar to normal background noise and can degrade all types of signals. Operators often mistake random noise jamming for receiver or atmospheric noise and fail to take appropriate electronic protection actions.
Stepped Tones	Tones transmitted in increasing and decreasing pitch. They resemble the sound of bagpipes. Stepped tones are effective against single-channel amplitude modulation or frequency modulation voice circuits.
Spark	Bursts are of short duration and high intensity; they are repeated at a rapid rate. This signal is effective in disrupting all types of radio communications. Spark jamming is easy to produce and one of the most effective jamming signals.
Gulls	Quickly rising and slowly falling variable radio frequency. The effect produced is similar to the cry of a seagull. Gulls produce a nuisance effect and are very effective against voice radio communications.
Random Pulse	Pulses of varying amplitude, duration, and rate. Pulses disrupt teletypewriter, radar, and various data transmission systems.
Wobbler	A single frequency, modulated by a low and slowly varying tone. The result is a howling sound that causes a nuisance effect on voice radio communications.
Recorded Sounds	Any audible sound, especially of a variable nature. Recorded sounds can distract radio operators and disrupt communications. Music, screams, applause, whistles, machinery noise, and laughter are examples.
Preamble Jamming	A tone resembling the synchronization preamble of the speech security equipment, broadcast over the operating frequency of secure radio sets. Results in all radios being locked in the receive mode. Preamble jamming is especially effective when employed against radio networks that use speech security devices.

Preventive Measures

A-26. Measures operators and planners can use to reduce susceptibility to enemy jamming include—

- Minimize radio transmissions, try to keep radio transmissions to six seconds or less.
- Use electronic counter-countermeasures, such as frequency hopping.
- Train using radio silence.
- Use low power setting on radios for normal operations to reduce the probability of detection.
- Use terrain masking to reduce the probability of detection and block potential sources of enemy jamming.

Indicators

A-27. The enemy strives to perfect and use new and more confusing forms of jamming, which requires radio operators to be increasingly alert to the possibility of jamming. Training and experience allow operators to determine whether a particular signal is a jamming signal. During operations, radio operators should remain alert to possible jamming indicators. Observable indications of jamming include—

- Apparently random noise or static over voice channels.
- Recorded sounds—messages or music—over voice channels.
- No answer to a radio transmission.

Reaction

A-28. Communications jamming requires prompt corrective action to restore critical communications capabilities. Possible reactions to jamming include—

- **Continuing to operate.** Enemy jamming usually involves a period of jamming followed by a brief listening period. Operator activity during this short period indicates to enemies whether their jamming efforts were successful. Continuing to operate normally gives the enemy no indication of success for failure. If the enemy hears discussion of the problem on the air, or radio operation terminates, the enemy may assume their jamming is effective. Operators should never terminate operation of a radio network unless ordered to do so. Operators should be careful not to disclose adverse effects of enemy jamming. This means normal operations should continue even when degraded by jamming.
- **Increasing transmitter power output.** Using low power for normal operations minimize the chance of detection. Once the enemy begins jamming the radios, the risk of detection becomes secondary to the radio delivering required communications. Higher radio power may overcome the enemy's jamming signal, but increases the risk of detection by enemy direction finding capabilities.
- **Improving the Signal-to-Jamming Ratio. The** signal-to-jamming ratio is the relative strength of the desired signal to the jamming signal at the receiver. If the desired signal is much stronger than the jamming signal, the jamming does not significantly degrade communications. To improve the signal-to-jamming ratio operators and signal leaders can consider the following—
- **Adjusting or changing the antenna.** When jamming occurs, the radio operator should adjust the antenna to receive the maximum incoming signal strength. Depending on the antenna, some methods include reorienting the antenna, changing antenna polarization at all stations, or installing an antenna with a greater range.
- **Establishing a retransmission site.** A retransmission site can increase the effective range and power of a signal between radio stations without increasing transmit power.
- **Relocating the antenna.** Operators may use terrain masking to block the incoming jamming signal. This may require relocating the antenna and associated radio set up to several hundred meters from its previous location.
- **Changing frequencies.** If a communications network cannot overcome enemy jamming, the commander may direct using an alternate or spare frequency. Preplanned and well-coordinated actions are required in order for practical dummy stations to continue to operate on the jammed frequency, to mask the change to an alternate frequency. During a jamming incident, it may be difficult to coordinate a frequency change. All radio operators require knowledge of when, and under what circumstances, they should switch to a backup frequency. If the frequency change is not smooth, the enemy may discover what is happening, and try to degrade communications on the new frequency.
- **Executing the primary, alternate, contingency, and emergency communications plan.** Quickly changing to the alternate or contingency means of communications reduces disruption of the command and control system.
- **Using signals intelligence or electronic warfare capabilities to locate the jamming signal.** Leveraging signals intelligence or electronic warfare capabilities requires coordination and collaboration with the G-2 (S-2) or the cyber electronic warfare officer.

A-29. If any of the corrective actions taken mitigate the enemy jamming, operators should continue operation of the network and submit a joint spectrum interference resolution report to higher headquarters. Joint spectrum interference reports document a history of problems and help identify possible causes for subsequent interference. Maintaining a historical record of interference helps develop countermeasures to future jamming incidents. Refer to ATP 6-02.70 for more information about joint spectrum interference resolution reporting.

Positioning, Navigation, and Timing Jamming

A-30. Peer threats have capabilities to contest the space domain and attack the on-orbit, link, and terrestrial segments of U.S. positioning, navigation, and timing satellites. These attacks may have significant impacts across all warfighting functions and many weapon platforms.

A-31. Electromagnetic jamming of positioning, navigation, and timing satellite capabilities affects not only communications, but also many other capabilities in tactical formations. Systems affected include—

- Communications systems.
- Friendly force tracking.
- Navigation.
- Reconnaissance.
- Radar systems.
- Precision guided munitions.

Preventive Measures

A-32. Measures to reduce susceptibility to, and mitigate the effects of, enemy jamming of positioning, navigation, and timing include—

- Using only encrypted positioning, navigation, and timing systems.
- Antenna masking.
- Terrain masking.
- Training and maintaining the ability to navigate using a map and compass.

Indicators

A-33. User indications that an enemy may be jamming positioning, navigation, and timing satellites include—

- Loss of satellite signal.
- Red Global Positioning System icon on the network management system.
- Loss of timing or incorrect time displayed on equipment.
- Wrong location displayed on the map.
- Jamming environment warning message.

Reaction

A-34. Because of the diverse and widespread effects of enemy positioning, navigation, and timing jamming, a prompt, coordinated response is necessary. Operators of all affected systems should—

- **Navigate using map and compass.** While this does not restore system timing and situational awareness displays, navigation using a map and compass cannot be jammed.
- **Increase distance between affected systems and jammer.** If the jammer operates from a known location, increased distance or terrain masking may mitigate interference.
- **Use signals intelligence or electronic warfare capabilities to locate the jamming signal.** Leveraging signals intelligence or electronic warfare capabilities requires coordination and collaboration with the G-2 (S-2) or the cyber electronic warfare officer.
- **Report jamming to higher headquarters.** Submitting a joint spectrum interference resolution report to higher headquarters documents a history of problems and helps identify possible causes for subsequent interference.

Satellite Communications Jamming

A-35. Expeditionary forces rely heavily on satellite communications capabilities for beyond line of sight network transport. Systems and capabilities affected by satellite communications jamming include—

- Friendly force tracking.
- Upper tier tactical internet.

- Tactical satellite radios.
- Intelligence reporting systems.

Preventive Measures

A-36. Operational and employment measures to prevent satellite communications jamming include—

- Minimizing transmissions on single-channel tactical satellite radios. Try to keep radio transmissions to six seconds or less.
- Terrain masking.
- Camouflage net masking.

Indicators

A-37. Possible operator indications of satellite jamming include—

- Seemingly random noise or static on single-channel tactical satellite radios.
- Recorded sounds, such as messages or music, over single-channel tactical satellite radios.
- No answer to transmission.
- Red satellite icon on network management system display.
- Loss of data from the satellite.
- Low signal-to-noise indicated on wideband satellite terminal.

Reaction

A-38. The reactive measures here apply mostly to narrowband (single-channel) satellite communications systems. When a single-channel tactical satellite radio operator recognizes a jamming attempt, they may—

- Increase radio transmit power. Only increase power on wideband satellite communications terminals if directed by the satellite controller.
- Change to a preapproved alternate frequency.
- Execute the primary, alternate, contingency, and emergency communications plan. Quickly changing to the alternate or contingency means of communications reduces disruption of the command and control system.
- Use signals intelligence or electronic warfare capabilities to locate the jamming signal. Leveraging signals intelligence or electronic warfare capabilities requires coordination and collaboration with the G-2 (S-2) or the cyber electronic warfare officer.
- Report jamming to higher headquarters. The higher headquarters' frequency manager and cyber electronic warfare officer can correlate reports from units across the area of operations to isolate enemy jammers and plan countermeasures, including nominating targets for lethal fires.
- Use line of sight systems for network transport. Units cannot communicate beyond line of sight, or through significant physical obstacles.

A-39. Satellite network controllers at the wideband satellite communications operations center coordinate all interference resolution and reporting on DOD wideband satellite networks. Refer to ATP 6-02.54 for more information about wideband satellite communications operations.

JOINT SPECTRUM INTERFERENCE RESOLUTION

A-40. Joint spectrum interference resolution reporting addresses electromagnetic interference and jamming incidents affecting the DOD. The objective of joint spectrum interference resolution is to document and assist in resolving electronic attack and recurring electromagnetic interference.

Incident Resolution

A-41. Frequency managers and electronic warfare Soldiers attempt to resolve incidents at the lowest possible level using organic assets. If the spectrum manager and cyber electronic warfare officer cannot

resolve an incident locally, they submit a joint spectrum interference resolution report through the chain of command. Each successive level attempts to resolve the incident before forwarding the report.

A-42. Corps and division spectrum managers coordinate regional and local interference resolution. The impact of each interference incident is unique, so no standard procedure establishes or guarantees resolution in every case. A systematic approach reduces the time and cost required to resolve interference situations. Refer to ATP 6-02.70 for more information about joint spectrum interference resolution reporting.

Reporting Procedure

A-43. Joint spectrum interference resolution reporting takes place through secure channels. Spectrum managers should not delay reports due to a lack of complete information. They can submit an initial report while attempting to resolve the incident, and follow-up reports to provide additional information, as it becomes available.

A-44. The submitter of a joint spectrum interference resolution report determines the appropriate security classification by evaluating the sensitivity of the electromagnetic interference on the affected system and considering the classification of the text comments.

A-45. Army units report through their chain of command up to the geographic combatant command, and to the United States Army Communications-Electronic Services Office. Message precedence of a joint spectrum interference resolution report depends on the urgency of the reported situation. Normally reports are routine or priority precedence, unless the originating unit believes the incident is hazardous to military operations. In this case, the unit reports using immediate precedence.

CYBERSPACE ATTACKS

A-46. U.S. networks face continuous risk of cyberspace attacks. Cyberspace risk increases substantially when operating against a peer threat in a contested environment. DODIN operations personnel implementing cybersecurity measures can prevent many attacks. If an enemy cyberspace attack breaches cybersecurity measures, it may require defensive cyberspace operations support to mitigate. Refer to FM 3-12 for more information about defensive cyberspace operations support.

Denial of Service

A-47. A denial-of-service attack seeks to make a computer or network resource unavailable to its intended users by disrupting services of a host connected to the Internet. An attacker floods the target computer or network resource with more requests than it can handle to overload the system and prevent it from fulfilling legitimate requests.

A-48. Denial of service attacks can affect any internet protocol network system, including—

- Mission command information systems.
- Logistics systems.
- Administrative systems.
- End user devices.

Preventive Measures

A-49. Good cybersecurity practices can prevent or lessen the effects of a denial of service attack. Cybersecurity personnel should—

- Maintain current anti-virus software and virus definition files.
- Maintain properly configured network firewalls.

Indicators

A-50. Operator indications of a denial of service attack may include—

- Unusually slow network performance when opening files or accessing websites.
- Request timeouts.
- Widespread unavailability of a website or network system.

Reaction

A-51. When faced with the symptoms of a denial of service attack, DODIN operations personnel should—

- Report to the next higher echelon G-6 (S-6) or joint force communications system directorate to determine whether the system slowdown is due to known activity on the network.
- Report suspected attacks to the G-2 (S-2) and G-3 (S-3).
- Continue operations using alternate or contingency communications means.

Malware

A-52. Malware is malicious software intentionally designed to damage a computer, server, or computer network. Malware attacks can affect any automated information system, including—

- Mission command information systems.
- Logistics systems.
- Administrative systems.
- End user devices.

Preventive Measures

A-53. Cybersecurity personnel attempt to prevent malware attacks by—

- Using and maintaining up to date anti-virus software and virus definition files.
- Creating and changing passwords according to the standards in Army Information Assurance Best Business Practices Document 04-IA-O-0001.
- Keeping system software updated and patched.
- Ensuring compliance with the most recent security technical implementation guidance.
- Maintaining properly configured network firewalls.

Indicators

A-54. Possible indicators of a malware attack include—

- Destruction or unexplained changes to files.
- Spontaneous restart of computers.
- Erratic, delayed, or unexpected computer or network activity.
- Anti-virus software warnings.

Reaction

A-55. If operators or DODIN operations personnel observe indications of a possible malware attack, they should—

- Report to the next higher echelon G-6 (S-6) or joint staff communication system directorate.
- Continue operations using alternate or contingency communications means.
- Report to G-2 (S-2) and G-3 (S-3).

A-56. DODIN operations personnel should not reconfigure computers or network systems in response to an attack unless directed by their next higher echelon.

Data Exfiltration and Collection

A-57. Data exfiltration may be either electronic—removing files through the network, or physical—removing paper or electronic copies from sensitive areas. Either method may disclose sensitive operational information and plans. Exfiltration of sensitive data may place operations at risk.

A-58. All automated information system are potential targets of data exfiltration and collection. Affected systems include—

- Mission command information systems.
- Logistics systems.
- Administrative systems.
- End user devices.

Preventive Measures

A-59. Cybersecurity measures and physical security combine to prevent data exfiltration and collection by—

- Implementing strict identity and access management controls for network systems.
- Enforcing strict physical security controls.
- Implementing access control restrictions.
- Employing data loss prevention software.
- Encrypting data-at-rest.
- Maintaining strong passwords for network access.

Indicators

A-60. Indicators of enemy data exfiltration and collection efforts include—

- Attempted or successful unauthorized physical access to sensitive areas.
- Unusually high volume of outgoing network traffic.

Reaction

A-61. The effects of data exfiltration can be catastrophic. If an enemy can steal enough documents, they can develop a complete assessment of U.S. capabilities, troop strength, logistics, and even operation plans. If any member of the unit suspects an enemy data exfiltration attempt, they—

- Report to G-2 (S-2) and G-3 (S-3).
- Report to next higher echelon.
- Consider changing the maneuver course of action if exfiltration compromises an operation or support plans.

Social Engineering

A-62. Social engineering uses techniques that rely on weakness in human nature rather than hardware or software. The goal is to deceive people into revealing passwords and other information that compromise the security of automated information systems and networks. Adversaries may also use social engineering techniques to identify and develop potential targets for phishing and spear phishing.

A-63. The target of a social engineering attack is an individual. A successful social engineering attack may compromise any system to which the affected individual has access.

Preventive Measures

A-64. All individuals should maintain operations security and cybersecurity awareness to avoid falling victim to a social engineering attack. They should—

- Confirm the identity of persons asking for personal information or access credentials.
- Pay close attention to website addresses.
- As a rule, individuals should avoid disclosing any information to unknown or unverified persons. Disclosing even seemingly innocuous information could make subsequent social engineering or spear phishing attempts against other targeted individuals seem much more legitimate.

Indicators

A-65. Indicators of social engineering attempts include—

- Unexpected phone calls from unknown callers requesting sensitive information.
- Websites that do not look normal, contain broken links, or have a mismatch between the text link and Internet address.
- Unauthorized personnel shoulder surfing.

Reaction

A-66. If personnel suspect a social engineering attempt, they should—

- Confirm the requestor's identity before disclosing information.
- Report the attempt to supervisors, network managers, and G-2 (S-2).
- Report social engineering attempts to next higher echelon.
- Promptly reporting attempts at social engineering can raise awareness and prevent others from falling victim to the same techniques.

Phishing and Spear Phishing

A-67. Phishing is a fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity in electronic communications. Spear phishing is a targeted phishing attempt, usually against key individuals or personnel with elevated or special access privileges.

A-68. Any individual may fall victim to a phishing attack. Key leaders and network administrators are also subject to spear phishing.

Preventive Measures

A-69. All personnel should protect themselves from phishing attacks by following best practices outlined in annual cybersecurity refresher training. Depending on the information operations condition level, the command may—

- Maintain awareness of the personal use of commercial e-mail.
- Restrict the use of personal e-mail, as required.
- Block access to commercial e-mail providers.

Indicators

A-70. Most common phishing techniques share certain traits, including—

- E-mails with generic greetings. Note that spear phishing attempts are likely be more refined and address the targeted individual by name.
- E-mails requesting personal information or login credentials.
- E-mails requesting or demanding an urgent response.
- E-mails with spoofed links—where the text displayed does not match the internet address shown when hovering over the link.

Reaction

A-71. If an individual suspects a phishing or spear phishing attempt, they should—

- Report the attempt to the chain of command, automation support section, and G-2 (S-2).
- Confirm the identity of the sender before taking any action.
- Individuals can further protect themselves from fraudulent links by never accessing their personal accounts through links in e-mails. For instance, if an e-mail purports to be from the individual's bank or credit card company, they should access their account only through the legitimate secure website, not through a hyperlink provided in an e-mail.
- Commands should not threaten punishment against individuals who inadvertently fall victim to phishing attempts. Fear of punishment could prevent individuals from reporting attacks.

Social Media Attacks

A-72. Adversaries may conduct social media attacks in support of their information collection and information operations goals. All individuals using any form of social media are potential targets.

Preventive Measures

A-73. Individuals should strictly limit personal information posted to their social media accounts. The compromise of this information could be damaging in itself or could strengthen an adversary's subsequent social engineering or spear phishing attacks.

A-74. Individuals should restrict who can view their social media profile and activities using the privacy settings on the social media platform.

A-75. Individuals and public affairs personnel must carefully weigh operations security considerations when they engage on social media platforms.

A-76. Individuals and group administrators should not accept friend or group membership requests from unknown or unverifiable persons.

A-77. Commands should consider limiting or restricting access to social media platforms as mission or operations security concerns dictate.

Indicators

A-78. Indicators of potential social media attacks include—

- Friend requests from unknown persons, or duplicate friend requests that mimic a known person.
- Unknown persons commenting on social media posts.

Reaction

A-79. If a social media attack is known or suspected, personnel should—

- Report the suspected compromise to the G-2 (S-2).
- Immediately change any compromised passwords.
- Watch for indicators of identity theft.

Attacks Against Personal Electronic Devices

A-80. Widespread use of personal electronic devices creates significant vulnerabilities when operating against a peer threat. Peer threats have demonstrated advanced capabilities to exploit personal electronic devices, seize control of cellular communications networks, and locate personal cellular phones with precision. This gives them the ability to collect information, conduct information warfare activities, and direct accurate lethal fires. Any personal electronic device capable of connecting to Wi-Fi, Bluetooth, or cellular communications systems is vulnerable to attack.

Preventive Measures

A-81. Measures to protect against personal electronic device attacks include—

- Maintaining strict control and accountability of personal electronic devices.
- Downloading only trusted apps from approved sources.
- Maintaining current security updates on devices and apps.
- Disabling Bluetooth and Wi-Fi features when they are not in use.
- Encrypting sensitive files and personal information.
- Allowing only government-provided personal electronic devices to connect to the DOD network.
- Commanders should consider restricting or banning the use of personal electronic devices, based on the tactical situation.

Indicators

A-82. Some possible indicators of attacks against personal electronic devices are—

- Enemy attacks that seem to correlate with personal electronic device usage.
- Incoming lethal attacks that occur with unexplained precision.
- Receiving a barrage of text messages—up to several per second—preventing the intended use of the device.
- Incoming propaganda or psychological warfare messages from unknown numbers.

Reaction

A-83. If a unit suspects it has come under attack, commanders should—

- Quickly displace the element under attack and direct all personnel to turn off personal electronic devices.
- Disable personal electronic devices and confiscate them, if necessary.
- Report to the next higher echelon.

This page intentionally left blank.

Appendix B
Maintenance

This appendix provides information and best practices on Army two-level maintenance and the communications-electronics maintenance and logistics processes that support tactical signal systems.

MAINTENANCE MANAGEMENT

B-1. Army organizations establish standard operating procedures and maintenance management processes to sustain, repair, evacuate, and report readiness status of critical communication systems. The Cyber Lessons and Best Practices Website contains sample maintenance standard operating procedures. Refer to FM 4-30 and ATP 4-33 for detailed information on maintenance support.

B-2. Communications-electronics maintenance must be a priority in the units' battle rhythm. By carefully managing scheduled and demand maintenance on signal equipment, units maintain visibility of the mission readiness of critical communications systems. Scheduled maintenance follows the schedule in the maintenance allocation chart in the equipment technical manual. Demand maintenance, or fault repair, is the process used by operators and maintainers to restore equipment to full functionality.

B-3. A maintenance plan should be a signed unit policy at the battalion level or higher. The maintenance plan outlines the separation in maintenance responsibilities in the unit, establishes a schedule for performing preventive maintenance checks and services on signal equipment, and clarifies the procedures to elevate maintenance issues to the appropriate maintenance support activity. Commanders should develop a maintenance focus based upon current operational challenges and maintenance trends. A deliberate, consistent, and engaged effort by all leaders is crucial to an effective maintenance plan.

B-4. Communications-electronics maintenance ensures WIN-T systems are mission ready. Signal operators perform preventive maintenance checks and services according to the operator's technical manual as scheduled maintenance. When equipment requires demand maintenance, operators troubleshoot the system to isolate the fault. In most cases, identified faults require a replacement line replaceable unit to correct the problem. Defined procedures for spare replenishment ensure replacement stock levels are adequate. The supporting communications-electronics maintenance shop maintains signal system spares, other than those identified in the end item component list as on-board spares. In order to maintain accountability, maintenance personnel track signal system spares in Global Combat Support System-Army as shop stock.

LIFE CYCLE MANAGED SYSTEMS

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

- Single-channel ground and airborne radio system.
- Joint Network Node.
- Command Post Node.
- Satellite Transportable Terminal.
- SMART-T.

NON-STANDARD EQUIPMENT

B-6. Non-standard equipment does not go through the formal life cycle management process because of an urgent need in supporting the unit's mission. Units acquire non-standard equipment to meet immediate operational needs through rapid fielding initiatives and urgent operational needs statements. Non-standard equipment is commercial off the shelf equipment such as—

- SIPR/NIPR access point.
- Deployable Ku band earth terminal.

TWO-LEVEL MAINTENANCE

B-7. The Army uses a tiered maintenance system consisting of field and sustainment maintenance. The goal of the maintenance system is to reduce repair times by repairing or replacing components, modules, or assemblies as close to the point of use as possible. Commanders, staffs, maintainers, and planners must understand two-level maintenance fundamentals in order to plan and execute their mission.

B-8. Field maintenance takes place at or near the point of use. Equipment operators, operator-maintainers, and ordnance-trained maintainers perform field maintenance on or near the system. The owning unit retains the equipment, or receives it back from the maintenance support facility when repairs are completed. Army maintenance units also provide field maintenance support.

B-9. Sustainment maintenance restores equipment to a national standard; after restoration, the equipment returns to the supply system. Sustainment maintenance requires evacuating the equipment to a support facility. When a unit sends equipment to a sustainment maintenance organization, the unit removes the equipment from its property book. Only in rare instances, such as unit reset, does the equipment return to the unit. The organic communications-electronics maintenance facility manages equipment exchanges and warranty actions. See table B-1 for the alignment of units to type of maintenance performed.

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

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

FIELD MAINTENANCE

B-10. Field maintenance consists of operator/crew maintenance and maintainer maintenance. Field maintenance restores unserviceable equipment using line replaceable unit or module replacement to make repairs. The owning unit normally performs field maintenance using organic tools and test equipment. Field maintenance is not limited to removal and replacement actions. If the operator, crew, or maintainer has the skills, special tools, repair parts, technical manuals, and time to repair an item, the unit should not evacuate equipment for sustainment maintenance.

B-11. Remark codes in the maintenance allocation chart explain each task, whether operator or maintainer. The maintenance allocation chart may indicate whether to evacuate an end item or service it on-site. If operators exhaust their troubleshooting and repair capabilities, they should request on-site support or equipment evacuation from the communications-electronics maintenance shop. The maintenance facility coordinates with the G-6 (S-6) for external technical support from United States

Army Communications-Electronics Command logistics assistance representatives or field service representatives.

B-12. Maintainers in the brigade support battalion support specialized organic equipment in the brigade combat team. These maintainers support the forward support companies, which are not structured to support system such as—

- Missiles.
- Fire control systems.
- Signal systems.

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

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

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

Operator and Crew Maintenance

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

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

Maintainer Maintenance

B-17. Ordnance Soldiers perform maintainer maintenance. Maintainers repair a component, accessory, assembly, subassembly, plug-in unit, shop replaceable unit, line replaceable unit, or other portion of the equipment, either on the system or after removal.

B-18. Depending on the system, the definition of a line replaceable unit or shop replaceable unit changes. The characterization of line or shop replaceable units for communications systems shifts as the level of troubleshooting increases in complexity. Maintainers at the infantry or Stryker brigade combat team support battalion communications-electronics shop have a network equipment support kit to perform limited functional checks, verify faults, and validate software and firmware versions before replacement actions.

SUSTAINMENT MAINTENANCE

B-19. Since field maintenance is closer to the point of use, it is the preferred method of repair. However, operators, crews, and unit maintenance personal sometimes lack the skills, special tools, repair parts, or authorization to complete repairs listed in the maintenance allocation chart. This may require evacuating

equipment for sustainment maintenance. Based on the damage or failure, leaders determine the best course of action, considering the operational and mission variables.

B-20. The intent of sustainment maintenance is to return items to a national standard, to provide a consistent and measureable level of reliability. Sustainment maintenance supports both operational forces and the Army supply system. Sustainment maintenance consists of—

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

COMMUNICATIONS-ELECTRONICS MAINTENANCE

B-21. The unique maintenance requirements of signal equipment and the need to maintain the DODIN-A with minimal downtime requires rapid maintenance response. Some operator-maintainers can perform more extensive field maintenance on their assigned equipment at the point of use. These operator-maintainers perform equipment replacement tasks to restore or maintain the DODIN-A.

NETWORK MAINTENANCE

B-22. Maintaining the DODIN-A requires continual coordination between signal leaders and staffs. G-6 (S-6) staffs collaborate across organizational boundaries to sustain their portions of the DODIN-A. Units must be capable of employing and maintaining their WIN-T equipment, and leveraging the technical expertise and knowledge of logistics assistance representatives and field service representatives as a part of their maintenance strategy.

B-23. The network management technician and the electronic systems maintenance warrant officer handle requests for external support of mission command information systems, tactical network systems, and tactical radios. This ensures centralized reporting and readiness efforts from United States Army Communications-Electronics Command, the brigade logistics support team, the regional support center, and contract field service representatives.

Communications-Electronics Maintenance in the Maneuver Battalion

B-24. The S-6 in coordinates with the logistics staff, communications-electronics maintenance facility, and the forward support company commander to develop a comprehensive maintenance plan supporting operations. The maintenance plan includes the complete process from preventive maintenance checks and service, fault identification, failed component removal and replacement procedures, and evacuation of equipment to communications-electronics support if required. The maintenance plan becomes part of the unit's maintenance standard operating procedure. This establishes responsibilities and procedures to preserve the battalion's maintenance readiness. Signal support systems specialists in the brigade and battalion S-6—

- Replace defective line replaceable units or modules in communications-electronics systems, communications security and transmission security devices, remote control systems, intercoms, and automated information systems.
- Schedule and annotate all scheduled services and demand maintenance in Global Combat Support System-Army, according to the equipment operator's manual.
- Replace line replaceable units or modules in faulted communications-electronics equipment and automated information systems or evacuates equipment to the forward support company for repair or replacement.
- Install and repair unit communications wiring and cabling.
- Install and remove vehicular and base station communications systems and automated information systems. This includes installation kits, antennas, and cabling on vehicular platforms.
- Test communications-electronics systems.
- Maintain test, measurement, and diagnostic equipment calibration records.
- Manage and maintain battery inventory and charging systems.
- Order and maintain bench stock.
- Apply modifications and directions, such as technical bulletin guidance.

B-25. Maneuver battalions typically receive field maintenance support from the brigade support battalion's forward support company. The forward support company maintenance platoon repairs automotive, armament, ground support, electronics, and missile equipment. The forward support company focuses on line replaceable units using combat spares from prescribed load list and shop stock. The forward support company service and recovery section performs battle damage assessment and repair. Most maintenance requests and evacuations for WIN-T systems pass through the forward support company directly to the field maintenance company communications-electronics maintenance shop.

B-26. The forward support company maintenance control section uses logistics automated information systems to order and track repair parts. The forward support company commander establishes maintenance collection points in coordination with the maneuver battalion's logistics staff.

Communications-Electronics Maintenance in the Brigade

B-27. The brigade S-6 maintains and monitors the status of the brigade's portion of the DODIN-A. The S-6 works closely with the brigade signal company commander, brigade engineer battalion staff, and the executive officer to ensure critical network maintenance and parts are available to support operations.

B-28. The S-6 maintains the communications status report as part of the signal running estimate. The communications status report shows the systems authorized, on-hand, and fully mission capable. The S-6 may tailor the communications status report to track only those systems the commander has prioritized. In addition to the S-6 communications status report, the staff reports status of life cycle managed systems through Global Combat Support System-Army and the unit status report. These two reports are key portions of a commander's view of unit readiness.

B-29. Maintenance managers should add pacing items and critical communications systems of systems to combat power reports to increase awareness of their mission criticality beyond the signal community. These reporting efforts and the increased emphasis drives maintenance priorities and enhances maintenance readiness. The brigade S-6 must clearly state the requirements for WIN-T spares and on-board spares to support maintenance demands.

B-30. 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 and the field maintenance company supports the brigade headquarters and other non-maneuver units in the brigade.

B-31. The field maintenance company base support platoon maintains electronics equipment and manages communications equipment float. The forward support company focuses on line replaceable units using combat spares from shop stock. The forward support company service and recovery section performs battle damage assessment and repair. The forward support company's maintenance control section uses logistics automated information systems to order and track repair parts. The forward support company commander establishes maintenance collection points in coordination with the brigade logistics staff.

Brigade S-6

B-32. The brigade S-6 closely tracks the maintenance status and availability of the brigade's communications equipment and systems. The brigade S-6 works closely with the brigade signal company commander, executive officer, and electronic systems maintenance warrant officer to verify performance of critical network maintenance and services, and to ensure sufficient repair parts and spares are available to preserve operational readiness. The S-6 should periodically review the equipment status report and order status report from Global Combat Support System-Army to maintain visibility of signal platform status and parts order status. The S-6 should ensure accurate inventories and validation of spares occur at least quarterly. WIN-T spares are accounted for on a component of end item hand receipt or as shop stock in the Global Combat Support System-Army.

Brigade Signal Company

B-33. The brigade signal company tracks network performance and maintenance issues in collaboration with the brigade S-6. Signal operator-maintainers perform field maintenance on the brigade's organic signal equipment. The signal company executive officer coordinates training and maintenance support for organic equipment, and maintains logistical and maintenance oversight for the company.

UNITS WITH NO ORGANIC MAINTENANCE CAPABILITIES

B-34. Some units in the brigade have limited or no organic field maintenance capabilities. These units normally receive field maintenance support or augmentation from a supporting maintenance organization. Maneuver battalions are examples of units without organic field maintenance capabilities. These units receive field maintenance support from the brigade support battalion's forward support companies. Functional brigades without organic maintenance capabilities normally coordinate for support from a sustainment brigade or combat sustainment support battalion. The sustainment brigade or combat sustainment support battalion's support maintenance company provides field maintenance to division and above units with no organic maintenance capabilities.

SPARES MANAGEMENT AND ACCOUNTABILITY

B-35. The organic communications-electronics maintenance element performs spares management for mission command information systems, network systems, and other signal platforms, with the exception of on-board spares designated as components of an end item. Central management of signal spares by the organic maintenance element expedites replacement of unserviceable items, enables fault verification, generates requisition demand history, and pools limited spares so they available across the command. If spares management is decentralized, the relatively lower local demand may not support retention of the spares as shop stock or authorized stockage list items.

B-36. Spares management affects various quarterly, semi-annual and annual services on major signal platforms. Communications-electronics technicians verify faults to avoid unneeded evacuation of spares without confirmed hardware, software or firmware faults. Evacuation of items with no evidence of fault wastes operational funds and reduces the pool of available spares. Global Combat Support System-Army can generate a supply demand history for spares, even if they are replaced under warranty or through standard requisition processes. The collection of demand history aids analysis of maintenance trends, helps identify systemic parts failures, and records line replaceable unit demand to inform procurement actions by the item manager.

B-37. Communications-electronics maintenance facilities can better manage spares and provide the flexibility to support various mission requirements at the company or team level. The S-6 collaborates with the S-3 and the electronic systems maintenance officer to tailor a logistics package to support training and operational missions. This allows for maintenance prioritization, balanced use of support, and efficient use of spares.

Physical Security of Spares

B-38. Physical security of signal spares remains an accountability concern, based on historical trends from the loss of program manager-issued spares. Maintenance plans must address securing, organizing, and protecting signal spares from in-transit damage. Table of organization and equipment-authorized storage containers may not be sufficient. With the steady influx of spares for all other systems, a formation's organic storage capacity is even more strained.

Mobility of Spares Storage

B-39. Units may require multiple lifts or be forced to prioritize movement of multiple spares containers. Lesson learned indicate commanders should consider procurement of additional Army-approved storage solutions to increase capacity. Portable, customizable containers or hardened transit cases with foam inserts are common storage options to mitigate capacity and mobility shortfalls.

Environmental and Weather Impacts Affecting Spares

B-40. Fully or partially environmentally controlled storage areas are essential in areas prone to extreme heat, humidity, and moisture. High cost, low density electronic and electrical components may fail after long exposure to harsh environments. Most WIN-T spares are sensitive to environmentally-induced failures due to corrosion or electrostatic discharge. Without deliberate measures to mitigate these conditions, spares may not be functional or available when needed. Commanders get increased operations and maintenance funding costs to replace environmentally damaged WIN-T spares never used.

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. Terms for which ATP 6-02.60 is the proponent are marked with an asterisk (*). The proponent publication for other terms is listed in parentheses after the definition. .

SECTION I – ACRONYMS AND ABBREVIATIONS

DISN	Defense Information Systems Network
DODIN	Department of Defense information network
DODIN-A	Department of Defense information network-Army
Eb/N0	energy per bit to noise power spectral density ratio
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-6	assistant chief of staff, signal
HF	high frequency
IP	Internet protocol
MAC	medium access control
NIPRNET	Non-classified Internet Protocol Router Network
NOSC	network operations and security center
S-2	battalion or brigade intelligence staff officer
S-3	battalion or brigade operations staff officer
S-6	battalion or brigade signal staff officer
SIPRNET	SECRET Internet Protocol Router Network
SMART-T	Secure Mobile Anti-Jam Reliable Tactical Terminal
TCN	Tactical Communications Node
UHF	ultrahigh frequency
VHF	very high frequency
VoIP	Voice over Internet Protocol
WIN-T	Warfighter Information Network-Tactical

SECTION II – TERMS

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)

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, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. 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)

Department of Defense information network operations

Operations to secure, configure, operate, extend, maintain, and sustain Department of Defense cyberspace to create and preserve the confidentiality, availability, and integrity of the Department of Defense information network. Also called **DODIN operations**. (JP 3-12)

electronic 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 electronic warfare support measures/signals intelligence without significantly degrading the operation of friendly systems. (JP 3-13.1)

enclave

A collection of computing environments connected by one or more internal networks under the control of a single authority and security policy. (CNSSI 4009)

information environment

The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. (JP 3-13)

local area network

A data communications system that (a) lies within a limited spatial area, (b) has a specific user group, (c) has a specific topology, and (d) is not a public switched telecommunications network, but may be connected to one. Note 1: Local area networks are usually restricted to relatively small areas, such as rooms, buildings, ships, and aircraft. Note 2: An interconnection of local area networks within a limited geographical area, such as a military base, is commonly referred to as a campus area network. An interconnection of local area networks over a city-wide geographical area is commonly called a metropolitan area network. An interconnection of local area networks over large geographical areas, such as nationwide, is commonly called a wide-area network. Note 3: Local area networks are not subject to public telecommunications regulations. (American National Standard T1.523.2011)

reachback

The process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed. (JP 3-30)

*** regional hub node**

The gateway transport node for the Warfighter Information Network-Tactical, and the transport medium for theater-based network service centers.

wide-area network

A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network and is usually spread over a larger geographic area than that of a local area network. Note 1: Wide-area networks may include physical networks, such as Integrated Services Digital Networks, X.25 networks, and T1 networks. Note 2: A metropolitan area network is a wide-area network that serves all the users in a metropolitan area. Wide-area networks may be nationwide or worldwide. (American National Standard T1.523.2011)

References

All URLs accessed on 12 July 2019.

REQUIRED PUBLICATIONS

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

ADP 1-02. *Terms and Military Symbols*. 14 August 2018.

DOD Dictionary of Military and Associated Terms. June 2019.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT PUBLICATIONS

Most joint publications are available online: https://www.jcs.mil/Doctrine.

DODI 8500.01. *Cybersecurity*. 14 March 2014.

DODI 8510.01. *Risk Management Framework for DOD Information Technology*. 12 March 2014.

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

JP 3-13. *Information Operations*. 27 November 2012.

JP 3-13.1. *Electronic Warfare*. 8 February 2012.

JP 3-30. *Command and Control for Joint Air Operations*. 10 February 2014.

JP 6-0. *Joint Communications System*.10 June 2015.

ARMY PUBLICATIONS

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

ADP 1. The *Army*. 17 September 2012.

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

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

ATP 3-37.34, *Survivability Operations*, 16 April 2018.

ATP 4-33. *Maintenance Operations*. 14 April 2014.

ATP 6-02.53. *Techniques for Single-Channel Radio Operations*. 7 January 2016.

ATP 6-02.54. *Techniques for Satellite Communications*. 5 June 2017.

ATP 6-02.70. *Techniques for Spectrum Management Operations*. 31 December 2015.

ATP 6-02.71. *Techniques for Department of Defense Information Network Operations*. 30 April 2019.

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

FM 3-12. *Cyberspace and Electronic Warfare Operations*. 11 April 2017.

FM 3-14. *Army Space Operations*. 19 August 2014.

FM 4-30. *Ordnance Operations*. 1 April 2014.

FM 6-02. *Signal Support to Operations*. 22 January 2014.

FM 6-27. *The Commander's Handbook on the Law of Land Warfare*. 7 August 2019.

OTHER PUBLICATIONS

American National Standard T1.523.2011. Alliance for Telecommunications Industry Solutions Telecom Glossary https://glossary.atis.org/.

Army Information Assurance Best Business Practices Document 04-IA-O-0001. *Army Password Standards*. 1 May 2008. https://www.milsuite.mil/book/servlet/JiveServlet/download/22894-1-114498/04-IA-O-0001_Army_Password_Standards.pdf.

CNSSI 4009. *Committee on National Security Systems (CNSS) Glossary*. 6 April 2015. https://www.cnss.gov/CNSS/issuances/Instructions.cfm.

RECOMMENDED READINGS

ADP 1-01. *Doctrine Primer*. 2 September 2014.

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

FM 3-94. *Theater Army, Corps, and Division Operations*. 21 April 2014.

JP 3-0. *Joint Operations*. 17 January 2017.

JP 3-14. *Space Operations*. 10 April 2018.

JP 3-33. *Joint Task Force Headquarters*. 31 January 2018.

WEBSITES

Army Centralized Army Service Request System https://acas.army.mil/. (Requires DOD-approved certificate login and user account).

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

DOD Cyber Exchange https://public.cyber.mil/stigs/. (Requires DOD-approved certificate login).

Joint Integrated Satellite Communications Tool portal (SIPRNET).

Project Manager Tactical Network Information and Support Exchange https://win-t.army.mil/wint/menu.cfm. (Requires DOD-approved certificate login and user account).

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

Unless otherwise indicated, DA Forms are available on the Army Publishing Directorate (APD) web site: https://armypubs.army.mil.

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

Index

Entries are by paragraph number.

ATP 6-02.60

9 August 2019

By Order of the Secretary of the Army:

JAMES C. MCCONVILLE
General, United States Army
Chief of Staff

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army
1921317

DISTRIBUTION:
Distributed in electronic media only(EMO).

PIN: 106015-000