FM 6-02

SIGNAL SUPPORT TO OPERATIONS

SEPTEMBER 2019

DISTRIBUTION RESTRICTION:

Approved for public release; distribution is unlimited.

This publication supersedes FM 6-02, dated 22 January 2014.

HEADQUARTERS, DEPARTMENT OF THE ARMY

Field Manual
No. 6-02

Headquarters
Department of the Army
Washington, D.C., 13 September 2019

Signal Support to Operations

Contents

*This publication supersedes FM 6-02, dated 22 January 2014.

Figures

Tables

This page intentionally left blank.

Preface

FM 6-02 is the highest-level signal doctrine manual. It describes how signal Soldiers support Army forces as they shape operational environments, prevent conflict, conduct large-scale combat operations, and consolidate gains against a peer threat in joint operations. In order to understand this publication, readers must be familiar with Army capstone doctrine (ADP 1 and ADP 3-0), ADP 5-0, ADP 6-0, and FM 3-0. FM 6-02 supports foundational Army doctrine and establishes context for signal-specific Army techniques publications.

FM 6-02 is applicable to all members of the Army Profession—leaders, Soldiers, and Army civilians. The principal audience for FM 6-02 is Army commanders, leaders, staffs, and signal Soldiers. Commanders and staffs of Army headquarters serving as a joint task force or multinational headquarters also use applicable joint or multinational doctrine for command and control of joint or multinational forces. Trainers and educators throughout the Army 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 according to 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.

FM 6-02 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. Terms for which FM 6-02 is the proponent publication (the authority) are marked with an asterisk (*) in the glossary. Definitions for which FM 6-02 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.

FM 6-02 applies to the Active Army, Army National Guard/Army National Guard of the United States, and the United States Army Reserve, unless otherwise stated.

The proponent for FM 6-02 is the United States Army Cyber Center of Excellence. The preparing agency is the Doctrine Division, 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 (FM 6-02), 506 Chamberlain Avenue, Fort Gordon, GA 30905-5735; by e-mail to usarmy.gordon.cyber-coe.mbx.gord-fg-doctrine@mail.mil.

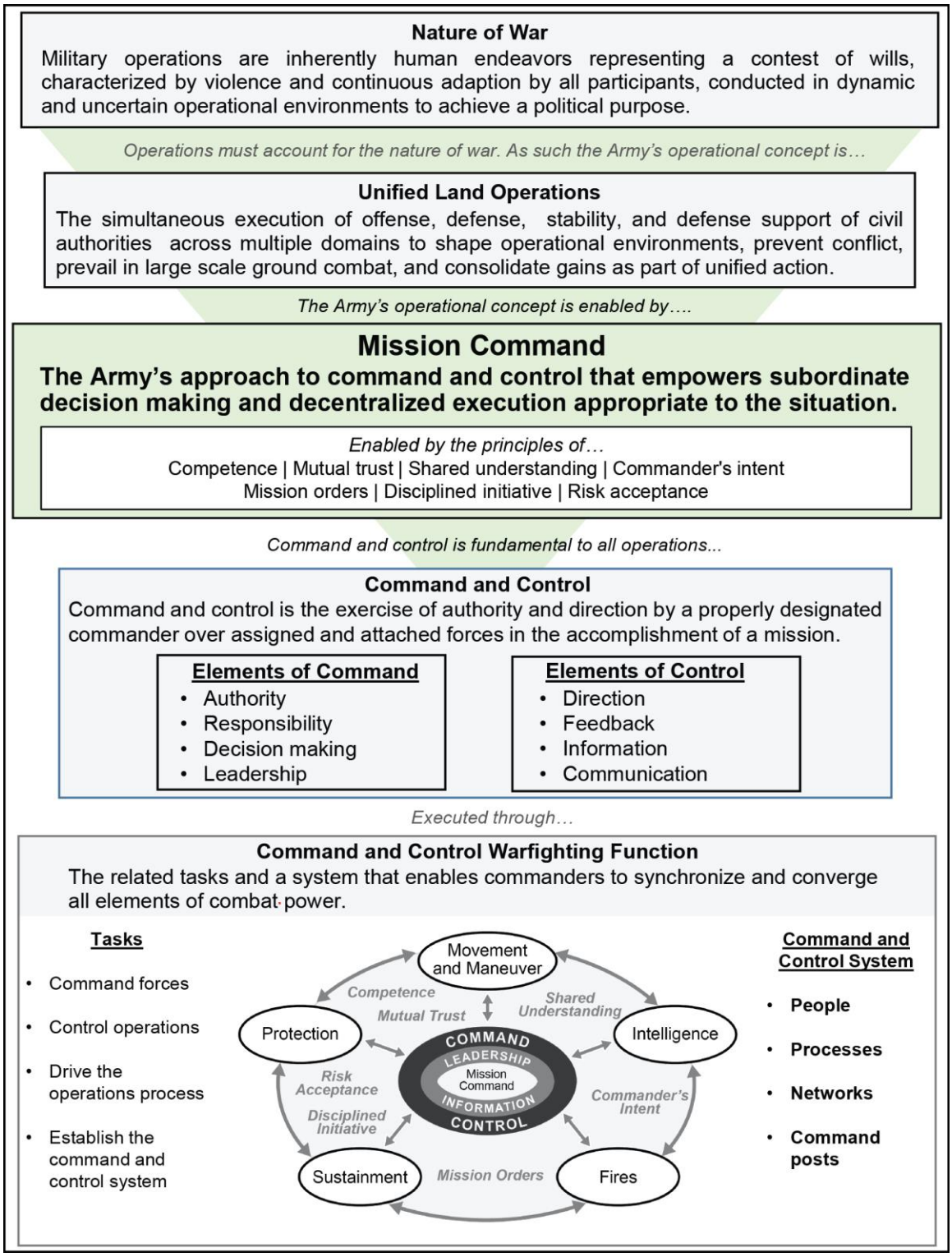
This page intentionally left blank.

Introduction

Command and control is fundamental to joint and Army operations. *Command and control* is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of a mission (JP 1). The Army's approach to command and control in unified land operations is mission command.

Mission command is the Army's approach to command and control that empowers subordinate decision making and decentralized execution appropriate to the situation (ADP 6-0). Mission command guides commanders, staffs, and subordinates in their approach to operations. The command and control warfighting function enables commanders and staffs of theater armies, corps, divisions, and brigade combat teams to synchronize and integrate combat power across multiple domains and the information environment.

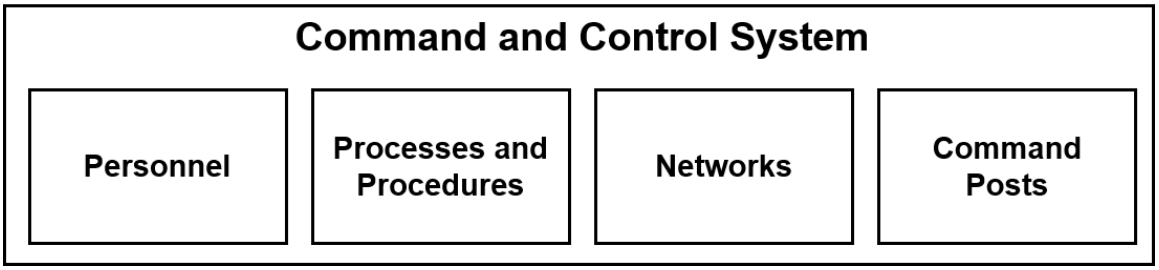
Commanders cannot exercise command and control alone. Commanders exercise command and control through the command and control warfighting function. The *command and control warfighting function* is the related tasks and a system that enable commanders to synchronize and converge all elements of combat power (ADP 6-0). See introductory figure-1 on page viii.



Introductory figure-1. Command and control logic map

A *command and control system* is the arrangement of people, processes, networks, and command posts that enable commanders to conduct operations (ADP 6-0). The command and control system enables the commander and staff to execute the command and control warfighting function. Signal forces provide the

network, information systems, and information management processes that enable command and control. Signal soldiers implementing the network and information systems and performing their staff tasks enable secure communications and situational awareness throughout their operational area. This enables the commander's exercise of command and control in support of unified land operations. See introductory figure-2.



Introductory figure-2. The command and control system

By providing the network and conducting information management tasks to support the knowledge management process in the command and control system, signal formations and staff elements enable secure communications and situational awareness throughout their areas of operations. Information management processes enable knowledge management and allow commanders to control their formations and synchronize efforts across warfighting functions while conducting unified land operations.

The Army's network enables every mission, from training the force to executing tactical tasks to influence the operational environment in large-scale combat operations. The network is the part of the command and control system that provides infrastructure for voice, data, and video connectivity to support operations. The network disseminates the common operational picture and enables unified action partner integration. With modern tactical radio systems able to pass digital information, the network extends as low as the individual Soldier on the battlefield.

FM 6-02 outlines signal doctrine in five chapters with supporting appendixes to address tactics and procedures for signal support to Army operations. The techniques to accomplish the signal missions, functions, and tasks in this field manual appear in signal-specific Army techniques publications.

This revision to FM 6-02 adopts new doctrinal terms, force structure, and tactics implemented since the most recent update. This manual supersedes FM 6-02, dated 22 January 2014. FM 6-02 chapters include—

Chapter 1 section I discusses the operational environment, information environment, and threat as they relate to signal support. Section II introduces the fundamental principles of successful signal support to joint and Army operations and the core competencies of the Signal Corps. Section III discusses the role of signal forces in Army operations.

Chapter 2 section I discusses signal support to Army operations by echelon—corps and below units with organic signal capabilities; units without organic signal capabilities; echelons above corps signal units that provide support; and signal support to other Army operations. Section II details the core competencies and essential capability of the Signal Corps. Section III discusses individual and collective signal training. Section IV discusses the joint and Army networks that enable command and control across the range of military operations.

Chapter 3 section I discusses signal support to Army operations to shape. Section II discusses signal support to Army operations to prevent.

Chapter 4 section I provides an overview of signal support to large-scale combat operations. Section II discusses signal support to large-scale defensive operations. Section III discusses signal support to large-scale offensive operations.

Chapter 5 discusses signal support to Army operations to consolidate gains.

Appendix A discusses tactics and procedures for operations in a contested environment. It outlines the procedures when communications systems and networks come under enemy electronic or cyberspace attack.

Appendix B discusses the role of the signal staff in the military decision-making process. It outlines the process and considerations for planning and coordinating Department of Defense information network operations, network transport and information services, spectrum management, and communications security.

Appendix C provides procedures for requesting visual information and combat camera support.

Appendix D discusses signal systems maintenance. It outlines two-level communications-electronics maintenance, the roles and responsibilities for maintenance management in units, and the external organizations that provide sustainment maintenance support.

Appendix E provides procedures for identifying support requirements and requesting signal support from non-organic assets.

Based on current doctrinal changes, certain terms for which FM 6-02 is the proponent have been modified for purposes of this publication. The glossary contains acronyms and defined terms. See introductory table-1 for specific term changes.

Introductory table-1. Modified Army terms

Term	***Remarks***
network transport	Modified definition

Pro Patria Vigilans! (Watchful for the Country)

Signal Corps Motto

Chapter 1
Overview of Signal Support

Signal personnel and units at all echelons provide and secure the network for their commanders to conduct command and control and integrate the other warfighting functions across the range of military operations. This chapter describes the operational environment, the fundamental principles and core competencies of signal support, and the role of signal forces in support of Army operations.

SECTION I – THE OPERATIONAL ENVIRONMENT

1-1. Threats to U.S. interests throughout the world are countered by the ability of U.S. forces to respond to a wide variety of challenges along a competition continuum that spans from cooperation to war. U.S. forces conduct a range of military operations to respond to these challenges.

1-2. Signal forces provide communications services that can quickly transition from fixed garrison infrastructure to deployed tactical systems to support Army commanders and units as they execute their assigned missions. The fixed infrastructure on posts, camps, and stations; mobile single-channel radio networks; and deployed communications sites combine to provide commanders the communications and information technology capabilities they need, at the right time and location, across the conflict continuum.

CHALLENGES FOR ARMY SIGNAL SUPPORT

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

1-4. Army forces participate in operations as part of a joint and multinational force. These operations serve a higher political purpose, and they should be planned and executed at each echelon to support that purpose (FM 3-0). Signal planners must include unified action partner interoperability in signal support plans to enable collaboration and synchronization with joint, interorganizational, and multinational mission partners.

1-5. Expeditionary forces must be ready to deploy on short notice to austere locations and immediately conduct combat operations. Commanders sequence their deployment so the arriving forces can defend themselves until follow-on forces arrive in the operational area. The earliest arriving forces have limited communications and network capabilities until their organic signal capabilities arrive and establish the network.

OPERATIONAL ENVIRONMENT OVERVIEW

1-6. Factors that affect operations extend far beyond the boundaries of a commander's assigned area of operations. Commanders and their staffs seek to develop and maintain an understanding of their operational environment. An *operational environment* is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). An operational environment encompasses physical areas of the air, land, maritime, and space domains, as well as the information environment, which includes cyberspace, the electromagnetic spectrum, and other factors. Threat, friendly, and neutral actors can all affect conditions in the information environment and, by extension, the operational environment. Because cyberspace and the electromagnetic spectrum span all physical domains and geographic areas, some of these effects may originate outside the area of operations.

Commanders face new challenges in defending capabilities in cyberspace where boundaries are far less identifiable. Attacks in cyberspace can originate from, and route through, friendly, neutral, and adversary countries.

1-7. As commanders operate across the range of military operations, signal capabilities must be tailorable to meet the commander's requirements. The way signal formations deliver communications services varies based on the mission. Communications requirements during theater security cooperation activities from fixed posts, camps, or stations differ from a brigade combat team commander's requirements during a movement to contact mission in large-scale combat operations. Signal staff officers and leaders need to clearly articulate to commanders what communications capabilities are available during critical points of an operation and how these capabilities support the exercise of command and control.

1-8. Understanding the operational environment is essential for signal leaders, engineers, planners, system operators, and cybersecurity professionals to plan and execute effective signal support. Signal Soldiers must understand signal flow from the end user, through the local area network, through the wide-area network, and the Department of Defense information network-Army (DODIN-A). The *Department of Defense information network-Army* is an Army-operated enclave of the Department of Defense information network that encompasses all Army information capabilities that collect, process, store, display, disseminate, and protect information worldwide (ATP 6-02.71). As an example, planners should understand how severe weather in Guam may affect satellite communications networks in Korea, or a cyberspace incident in the continental United States can quickly traverse the network and affect communications in an operational theater.

INFORMATION ENVIRONMENT

> *"There is no better example of the challenge ahead than that of the information environment. From moving supplies in the wake of a hurricane disaster to ordering troops to the Pacific, or addressing the ever-changing cyber[space] threat, the global dependence on information and networks in everyday activities demands our attention now."*
>
> —General Martin E. Dempsey, former Chairman of the Joint Chiefs of Staff

1-9. Across the globe, information is increasingly available in near-real time. The DODIN-A provides the ability to access this information from anywhere, and at any time. Access to information enables decision making, leadership, and combat power. It is also key to seize, gain, and retain the initiative and to consolidate gains in the operational environment.

1-10. 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). In modern conflict, controlling the information environment is as important as controlling key terrain in the physical domains. The information environment is not separate or distinct from the operational environment, but an integral part of it. Any activity that takes place in the information environment affects one or more of the warfighting domains.

1-11. Cyberspace and the electromagnetic spectrum are parts of the information environment. *Cyberspace* is a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (JP 3-12). Friendly, enemy, adversary, and host-nation networks, communications systems, computers, cellular phone systems, social media, and communications infrastructure are all parts of cyberspace.

1-12. The *electromagnetic spectrum* is the range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands (JP 3-13.1). The electromagnetic spectrum crosses all domains and provides the vital link between space and cyberspace domains. Cyberspace and the electromagnetic spectrum have become increasingly congested and contested, even as their importance to successful operations has increased. Army forces must be able to effectively operate in cyberspace and the electromagnetic spectrum while controlling the ability of enemies and adversaries to operate.

1-13. Signal Soldiers install, operate, and secure the DODIN-A in locations where both friendly and enemy cyberspace operations occur. Given the high risk to the network, signal operators and information system

users must continuously manage risk and secure their portions of the DODIN-A. Signal planners and DODIN operations personnel assess security risk during network design, mitigate risk in software employment, and continuously monitor for signs of malicious activity within the network. Individual users must maintain cybersecurity awareness and learn to identify signs of malicious activity. While cybersecurity efforts cannot prevent every intrusion, commanders and their staffs must take steps to identify, prioritize, and secure their most important networks and data.

1-14. Unlike the air, land, maritime, and space domains, cyberspace has no range constraints. A threat actor can disrupt, destroy, or intercept the flow of information while operating from the other side of the world. For example, in 2014, North Korea allegedly conducted cyberspace attacks against the California headquarters of Sony Pictures in retaliation for releasing a movie that insulted North Korean leaders. A peer threat or other adversary could recruit hackers around the world to attack Army capabilities within an area of operations, or all the way back to the strategic support area in the United States.

TRENDS

1-15. Proliferating technologies will continue to present challenges for the joint force. The widespread availability of inexpensive communications devices allows threat actors to greatly increase their command and control capabilities. Adversaries take advantage of the low entry cost to achieve offensive cyberspace capabilities. Cyberspace attacks are a low-cost means for state and non-state threat actors to attack civilian, military, and governmental targets. Cyberspace attacks can extend an enemy's reach. Enemies will use cyberspace attacks to counter the Army's dominance on the battlefield. Enemy forces no longer need to develop costly aircraft, naval, or missile systems to cause significant damage to infrastructure, command and control nodes, or logistic capabilities.

1-16. As technology continues to advance, so does the Army's reliance on the DODIN-A. Every aspect of Army operations relies on networked communications, from individual Soldiers, to logistics, precision fires, and command and control. In 2002, maneuver units' manning and equipment authorizations provided networked communications capabilities to echelons brigade and above, with limited satellite communications assets pooled at the division and corps. A typical 20–30 vehicle convoy included only three or four single-channel radios.

1-17. By 2005, satellite-based networked communications became available as low as battalion level. Nearly every vehicle now has a radio and some form of networked friendly force tracking capability. The increase in communications capabilities enables greater dispersion of forces and allows smaller forces to operate across a larger battlespace. The increased capabilities enable faster flow of information between commands, better flow of intelligence, just in time logistics, and enhanced situational understanding.

1-18. Over-reliance on technology creates significant vulnerabilities. Command and control nodes have always been key targets for enemy attack. An enemy can attack command and control nodes with lethal fires, cyberspace attack, or electronic attack. Army units have come to rely on uninterrupted, high-speed digital communications and satellite positioning, navigation, and timing. Units must be able to operate without these capabilities.

1-19. Soldiers need the skills to navigate with a map and compass to operate when capabilities are degraded or denied. Staffs need to maintain paper maps and overlays in command posts to maintain situational awareness of their area of operations if mission command information systems become disrupted or unavailable. A primary, alternate, contingency, and emergency (PACE) communications plan provides redundant communications means if the primary capability is unavailable. Disciplined initiative according to the commander's intent allows units to continue operations in the absence of reliable communications.

1-20. Peer threats have advanced capabilities to locate the electronic signature of communications systems. The cyber electronic warfare officer can help formulate communications and electronic protection plans to minimize the electronic signature of command posts and signal sites. Commanders should consider locating communications transmitters and antennas remotely from major command posts to protect the headquarters in case an enemy targets communications systems with lethal fires. Command posts and communications systems must frequently displace during large-scale combat operations against a peer threat.

Note. Locating a signal site remotely creates additional force protection and physical security requirements to secure and defend the remote site.

MULTI-DOMAIN EXTENDED BATTLEFIELD

1-21. Army forces both depend upon and enable the joint force across the air, land, maritime, space, and cyberspace domains. All Army operations are multi-domain operations and all battles are multi-domain battles. Conventional Army multi-domain operations include airborne and air assault operations, air and missile defense, cross-domain fires, aviation, electronic warfare (EW), cyberspace operations, military deception, information operations, military information support operations, information collection, and riverine operations. Since joint or multinational partners may provide some of these capabilities, Army commanders and staffs plan, coordinate, and integrate joint and other unified action partner capabilities in their multi-domain approach to operations. Large-scale combat operations require synchronization and convergence of capabilities and effects across multiple disciplines and domains.

1-22. Army forces may conduct operations across multiple domains to gain freedom of action for other members of the joint force. The air, land, maritime, space, and cyberspace domains, and their effects on the information environment are closely interrelated. Their complex relationships require a cross-domain understanding of the operational environment. Signal leaders must understand the available communications capabilities and interoperability challenges of communications support in each domain. A thorough understanding helps identify opportunities for the command to coordinate with unified action partners and converge effects when operating throughout the multi-domain battlefield.

1-23. Signal support is a key enabler for multi-domain battle. Signal units have effectively integrated communications capabilities across the air, land, maritime, space, and cyberspace domains for decades. The DODIN-A and the services it extends enable collaboration and synchronization across domains and among unified action partners.

SIGNAL DEPENDENCE ON SPACE-BASED CAPABILITIES

1-24. Signal support depends on access to space capabilities. Nearly all advanced countries and their military forces rely heavily on space-based capabilities in the areas of—

- Communications.
- Positioning, navigation, and timing.
- Detection and monitoring.

1-25. Peer threats will likely attempt to jam or destroy space-based capabilities as a means of disrupting U.S. operations. Disruption of positioning, navigation, and timing negatively impacts network synchronization, friendly force tracking, precision munitions, unmanned aircraft systems, and ground movements. Destroying or jamming satellite communications could reduce Army commanders' ability to exercise command and control beyond line of sight or in rugged or urban terrain. Exercising disciplined initiative with clear commander's intent, along with robust terrestrial-based communications capabilities, mitigates the disruption of space-based communications.

1-26. U.S. space capabilities include—

- Information collection.
- Early warning.
- Environmental monitoring.
- Satellite communications.
- Positioning, navigation, and timing.

1-27. Satellite communications enable beyond line of sight communications without terrain restrictions. Satellite-based positioning, navigation, and timing provides an accurate, universal source for system timing and location.

1-28. Space-based capabilities enable signal units to establish communications networks, navigate, and synchronize network systems. To most effectively employ space-based capabilities, signal Soldiers must understand the capabilities and how to coordinate access. Spectrum managers and signal planners at brigade and higher echelons assist units in planning, integrating, and coordinating access to satellite communications capabilities. Refer to FM 3-14 more information on Army space operations.

1-29. The proliferation of advanced technology provides more widespread access to space-enabled capabilities. Most potential adversaries have access to space-enabled technologies or the ability to degrade U.S. space capabilities. Commanders and signal leaders cannot assume they will retain unrestrained access to space-based capabilities. Units must prepare and train to conduct operations with degraded or disrupted capabilities.

1-30. Signal planners must understand the limitations of satellite communications systems. Communications links using multiple satellites and earth terminals introduce latency problems that interfere with Internet protocol routing. Signal operators and planners must understand satellite latency and its effects on the network. Applications that do not tolerate satellite latency, such as voice and video services, suffer degradation. Planners must design network plans to minimize latency.

CONGESTED ENVIRONMENT

1-31. Today, all joint force operations depend on assured electromagnetic spectrum access throughout the operational environment (JP 6-0). All forces and supporting agencies depend on the electromagnetic spectrum for communications, information collection, and EW capabilities in support of operations in the air, land, maritime, space, and cyberspace domains. Signal systems rely on the electromagnetic spectrum for network transport. For this reason, gaining and maintaining access to the electromagnetic spectrum is critical for signal support to joint and Army operations.

1-32. 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). Competition for the finite available bandwidth results in a congested electromagnetic spectrum, especially when operating in developed nations.

1-33. The proliferation of transmitting devices throughout an operational environment intensifies competition for bandwidth in the electromagnetic spectrum, complicates unified action partner interoperability, and increases the complexity of friendly networks. The vast number and variety of radio frequency transmitting devices in military and civilian use compounds the competition for electromagnetic spectrum access among the Army, the joint force, and the civilian population. At the same time, widespread use of commercial communications devices allows adversaries to mask their communications transmissions among the many other transmitters.

1-34. Signal staffs plan communications and network capabilities to support all anticipated requirements in their operational area. However, in a congested electromagnetic operational environment, there might not be adequate satellite bandwidth and spectrum availability to support all missions. Signal leaders must be able to clearly articulate the limitations and expected level of degradation, so commanders can make appropriate risk decisions and align the available capabilities with their priorities.

CONTESTED ENVIRONMENT

1-35. Enemies and adversaries may deliberately attempt to deny friendly use of the electromagnetic spectrum, space, cyberspace, and/or terrestrial systems. Due to heavy joint reliance on advanced communications systems, such an attack may be a central element of any enemy or adversary antiaccess 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).

1-36. Threat cyberspace and EW capabilities jeopardize U.S. freedom of action in cyberspace and the electromagnetic spectrum. Because communications are a key command and control enabler, U.S. military communications and information networks present high-value targets. Peer threats and other adversaries understand the extent of U.S. forces' reliance on communications and automated information systems.

Enemies and adversaries are likely to contest the information environment across the conflict continuum to deny operational access and diminish the effectiveness of U.S. and allied forces.

1-37. An enemy can use radio frequency direction finding equipment to locate any radio frequency emitter, such as a radio, satellite communications terminal, counter-improvised explosive device system, radar, or cell phone. Once they determine an accurate location, enemy forces can direct lethal or non-lethal fires to destroy, degrade, or compromise the capability.

1-38. Combining signal and electronic protection techniques with current intelligence estimates may mitigate an enemy's ability to find and attack key communications nodes or command posts. The assistant chief of staff, intelligence (G-2) or battalion or brigade intelligence staff officer (S-2) section can better define an enemy's electronic technical data. The cyber electronic warfare officer's knowledge of threat EW capabilities and techniques helps inform a communications plan to limit the enemy's effectiveness. Units can camouflage their operational use of the spectrum within the spectral noise of an urban area or mask communications transmissions using terrain or antenna placement. Refer to Army doctrine for EW and ATP 6-02.53 for more information about communications masking and antenna placement.

1-39. Synchronizing signal support with cyberspace, EW, intelligence, space, and other information-related capabilities is key to achieving and maintaining freedom of action in contested cyberspace and the electromagnetic spectrum while denying the same to adversaries. *Synchronization* is the arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time (JP 2-0). Synchronization provides the ability to execute multiple related and mutually supporting tasks in different locations at the same time, producing greater effects than executing each in isolation. Synchronization of capabilities across multiple domains and warfighting functions maximizes their complementary effects in and through cyberspace and the electromagnetic spectrum.

1-40. 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) could change communications requirements beyond the capabilities of assigned and attached signal elements. Because DODIN operations authorities align to the operational chain of command, commanders can allocate the available communications and network support to their highest mission priorities until additional capabilities are available. Refer to FM 6-0 for a complete discussion of the operational and mission variables.

Degraded Environment

1-41. The cyberspace and space domains grow in importance as global competitors, regional competitors, and non-state actors invest in capabilities to protect their access and disrupt or deny access to others. Although Army forces have grown accustomed to communicating freely without fear of jamming or interception, U.S. enemies and adversaries are likely to use technological advances in cyberspace and vulnerabilities in the electromagnetic spectrum to conduct cyberspace or electromagnetic spectrum attacks (FM 3-0).

1-42. A broad array of threat actors will challenge the joint force's freedom of action in space, cyberspace, and the electromagnetic spectrum. For example, an enemy that jams positioning, navigation, and timing satellites may render precision fires inaccurate. Army commanders must protect their own systems and disrupt the enemy's ability to operate while being prepared to operate with degraded communications and reduced access to cyberspace and space capabilities.

1-43. While enemy action might cause a degraded environment, degraded capabilities may also occur because of insufficient resources to support all communications requirements. For example, inadequate communications satellite capacity in an operational area cause congestion and network latency. Jamming or unintentional electromagnetic interference may also cause degradation. The architecture of the tactical network implements redundant communications means to improve reliability in a degraded environment.

1-44. In a hostile EW environment where satellite links are denied or degraded, Army forces at echelons corps through brigade retain the ability to communicate through protected satellite communications. Units at echelons battalion and below rely on line of sight communications and other terrestrial means to overcome satellite denial or degradation. Ground and aerial retransmission links can extend the communications range, but are still vulnerable to direction finding and jamming. Refer to ATP 6-02.54 for more information about protected satellite communications.

1-45. Careful operational planning can minimize disrupted operations in a degraded environment. The commander's priority of effort includes priorities of service. Continuity of operations plans, PACE plans, and disciplined initiative under the mission command approach can mitigate the effects of degraded communications capabilities. The information and knowledge management plans should include priorities for knowledge management in a degraded environment.

Denied Environment

1-46. Enemies and adversaries may adopt an antiaccess and area denial strategy against U.S. forces. An enemy or adversary with the ability to field layered and fully integrated antiaccess and area denial capabilities may try to deny U.S. access to an operational area altogether. Operations relying on the DODIN, and operations of the DODIN itself, must continue even in times of crisis. The DODIN architecture supports continued operations in a denied environment.

1-47. Continuity of operations plans, disaster recovery plans, and distributed DODIN operations reduce the adverse effects of isolated network disruptions. Network failures should be transparent to end users. Continuing operations rely on systems and capabilities that automatically and immediately transfer to alternate means, to minimize interruptions to connectivity. Denied access in an isolated area or operational theater does not affect the continued overall operation of the DODIN outside the contested area. See appendix A for more information about operations in a contested environment.

Continuity of Operations Planning

1-48. Army units must develop, train, and implement techniques across all warfighting functions to ensure continuity of operations and enable an accurate common operational picture when communications become degraded. These methods include—

- Anticipating and recognizing degraded and denied communications so operators can quickly employ countermeasures.
- Adjusting the dispersion of units.
- Graphic control measures.
- Bandwidth management.
- Adjusting operational tempo.
- Centralizing or decentralizing key communications capabilities, as required.
- Employing redundant communications, targeting, and collection assets.
- Implementing procedures to transfer critical data and information, both manually and verbally.
- Retaining the ability to perform critical command and control and other warfighting function tasks manually.
- Establishing push, versus pull, reporting procedures in case normal reporting is hindered.
- Planning locations and capacity for data storage.
- Scheduling regular backups of operational data.
- Establishing and rehearsing procedures for emergency restoration.

1-49. U.S. forces' increased reliance on reachback information and network capabilities creates vulnerabilities to attack from various sources. Employment of the mission command philosophy is essential to overcome the fog and friction that a decentralized, disaggregated, and degraded communications environment adds to the battlefield when other defensive countermeasures fail (FM 3-0). The assistant chief of staff, signal (G-6) or battalion or brigade signal staff officer (S-6) supports the assistant chief of staff, operations (G-3) and battalion or brigade operations staff officer (S-3) continuity of operations plans by planning a robust communications network with redundant means of transport and developing PACE plans during the military decision-making process.

Primary, Alternate, Contingency, and Emergency Plan

1-50. Commanders must be able to communicate with adjacent units, supporting joint forces, and host-nation and multinational forces in addition to their subordinates. Successful commanders understand that networks may be degraded through threat or environmental factors during operations. They develop methods and

measures to mitigate the impact of degraded networks (ADP 6-0). A PACE plan provides predictability and redundancy for communications in congested or contested environments. Redundant communications systems and methods enable communications throughout the corps and division areas of operations in contested environments. A viable, effective PACE plan may be the most valuable contribution of a G-6 (S-6) in the planning process.

1-51. A PACE plan is a key requirement for operations in a contested environment. Leaders need to be able to command their formations when communication networks are disrupted, while on the move, and without perfect situational awareness (FM 3-0). Continuous mission command requires adequate, but not necessarily continuous, network connectivity. PACE plans provide prioritized options for redundant means of communication to ensure effective command and control and interoperability:

- **Primary**—the best, and intended, method of communications.
- **Alternate**—another common, but perhaps less optimal method.
- **Contingency**—method may not be as fast, convenient, or reliable, but it can still accomplish the task.
- **Emergency**—communications method of last resort. Emergency methods may cause delays or otherwise affect operations.

1-52. Most units establish two PACE plans—one for communications to higher headquarters and one for subordinate units. The higher headquarters usually establishes the PACE plan for communications between echelons. Units should validate the PACE plan during mission rehearsals to ensure each means of communication is viable and to establish triggers for execution. Viable PACE plans are critical to support command and control in a degraded or denied environment. For a PACE plan to be viable, each method of communication must be feasible, suitable, acceptable, distinguishable, and complete. If a subordinate unit does not have the required equipment or is untrained in employing a system, that system should not be part of the PACE plan. See appendix B for more information about PACE planning.

THREAT EFFECTS ON SIGNAL SUPPORT

1-53. A *threat* is any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland (ADP 3-0). Threats can be categorized as adversaries, enemies, or insiders. An *adversary* is a party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged (JP 3-0). An *enemy* is a party identified as hostile against which the use of force is authorized (ADP 3-0). Insider threats present unique challenges because they are trusted individuals with access to Army capabilities and sensitive operational information. The primary threat context in FM 6-02 is peer threats in large-scale combat operations. See paragraph 1-90 for more information about insider threats.

PEER THREAT

1-54. A peer threat is an adversary or enemy with capabilities and capacity to oppose U.S. forces across multiple domains world-wide or in a specific region where they enjoy a position of relative advantage. Peer threats possess roughly equal combat power in geographical proximity to a conflict area with U.S. forces. Peer threats generate tactical, operational, and strategic challenges that are an order of magnitude more challenging militarily than those the U.S. Army has faced since the end of the Cold War (FM 3-0). Peer threats employ their resources across multiple domains to exploit U.S. vulnerabilities. They use their capabilities to create lethal and nonlethal effects across the operational environment. Peer threat tactics include preclusion, isolation, sanctuary, and systems warfare.

1-55. Peer threats have demonstrated advanced capabilities in long-range precision fires, integrated air defense, and EW. These threat capabilities demand changes to signal tactics, techniques, and procedures to counter the risks they present. Command and control nodes must displace frequently during large-scale combat operations to avoid destruction by enemy fires.

1-56. Peer threats consider U.S. communications, command and control nodes, massed formations, and critical infrastructure key targets during large-scale combat operations. Commanders should ensure as much dispersion of their formations as tactically prudent. Locating radio frequency emitters, such as satellite

communications antennas and line of sight radio systems away from major command posts minimizes loss of life and command and control capabilities if the enemy targets the communications systems with lethal fires.

Preclusion

1-57. Peer threats use a wide variety of capabilities to preclude a friendly force's ability to shape the operational environment and mass and sustain combat power. Antiaccess and area denial are two such activities. (FM 3-0). Regional peers will use their relative advantages in a geographic area to attempt to prevent U.S. forces from gaining operational access.

1-58. Peer threats will use cyberspace attacks and EW as part of their antiaccess and area denial strategy. Overcoming enemy antiaccess and area denial requires a forcible entry operation. Signal support to forcible entry operations (see paragraph 1-185) allows the joint force commander to synchronize maneuver and effects across multiple domains to gain a foothold from which to conduct land operations in the joint operations area. Refer to JP 3-18 for doctrine on joint forcible entry operations.

Isolation

1-59. Isolation is containment of a force so it cannot accomplish its mission. Peer threats believe that the defeat of the U.S. forces lies not at the end of a substantial battle, but through the culmination of U.S. efforts before U.S. goals are reached. In large-scale combat operations, peer threats will seek to isolate U.S. tactical forces and prevent their mutual support while threat forces work toward their campaign objectives. Some examples of how isolation may affect signal support are—

- Preventing or limiting communications with other units.
- Deceiving friendly forces as a means to gain access to the U.S. network.
- Targeting command and control nodes with lethal fires.
- Conducting denial of service attacks against the U.S. network.
- Electronic attack (jamming) to prevent U.S. and allied use of the electromagnetic spectrum.
- Denying satellite access through jamming or destruction of satellite communications capabilities.

1-60. The tactical network provides redundant means of network transport to prevent formations from becoming isolated. PACE communications plans and disciplined initiative within the commander's intent further mitigate the effects of isolation.

Sanctuary

1-61. Sanctuary is a threat method of putting threat forces beyond the reach of friendly forces. It is a form of protection derived by some combination of political, legal, and physical boundaries that restrict freedom of action by a friendly force commander. Peer threats will use any means necessary, including sanctuary, to protect key elements of their combat power from destruction, particularly by air and missile capabilities (FM 3-0).

1-62. Signal support enables information collection and disseminates the common operational picture, enabling commanders and their staffs to maintain situational understanding and support the targeting process throughout their area of operations. Comprehensive understanding of the threat force's position and situation reduces the protection they seek to derive by operating from sanctuary.

Systems Warfare

1-63. Peer threats view the battlefield, their own instruments of power, and an opponent's instruments of power as a collection of complex, dynamic, and integrated systems composed of subsystems and components. Peer threats use systems warfare to identify specific critical capabilities for disruption or destruction in order to cause failure of a larger friendly system (FM 3-0).

1-64. An example of systems warfare that affects signal support is an enemy using radio frequency direction finding to locate a critical retransmission site. Once the enemy locates the retransmission site, they can confirm the location using unmanned aircraft systems and direct long-range precision fires from sanctuary to

prevent counterattack. Targeting a critical retransmission asset has a more significant effect than destroying a typical single node in the network. Loss of the retransmission capability disrupts communications for many radios across a wide section of the area of operations. Refer to TC 7-100.2 for an in-depth discussion of systems warfare.

HYBRID THREAT

1-65. A *hybrid threat* is the diverse and dynamic combination of regular forces, irregular forces, terrorists, or criminal elements acting in concert to achieve mutually benefitting effects (ADP 3-0). Some aspects of the hybrid threat, such as criminal or terrorist organizations, do not abide by the law of war. Hybrid threats seek to exploit asymmetric advantages over an adversary to avoid engaging in direct combat.

1-66. In many ways, hybrid threat is not a new way of fighting a war; it is simply a new way of framing the operational environment. The Colonials in the American Revolution employed a hybrid strategy with a mixture of regular Continental troops, state militias, irregular partisans, and supportive local populations, along with publishers and pamphleteers sympathetic to the revolutionary cause. What has changed is the tools available to threat actors and the ability of some of these tools to create far-reaching effects outside the operational area. Enemies may employ cyberspace attack and exploitation, battlefield jammers, and space-based capabilities, such as anti-satellite weapons, to disrupt U.S. communications; positioning, navigation, and timing; synchronization; and freedom of maneuver. A peer threat's ability to combine regular and irregular forces, robust information warfare capabilities, long-range precision fires, and massed lethal fires with the capacity to contest or achieve air superiority presents a formidable challenge.

1-67. The hybrid threat understands that the most challenging environment for U.S. forces is one where conventional military operations occur in concert with irregular warfare. The hybrid threat concept is not simply making do with what is available, but deliberately taking advantage of all tools at hand to create a complex operational environment.

1-68. Hybrid threats employ a wide variety of military, paramilitary, insurgent, criminal, and information warfare capabilities in concert with a robust antiaccess and area denial strategy and long-range precision fires to support their strategic and tactical objectives. Each component of the hybrid threat brings additional capabilities to bear. Commanders should not underestimate the synergy of these capabilities. Operational environments are inherently complex due to the operational variables. The hybrid threat seeks to introduce additional complexity using an ever-shifting array of forces, technologies, and techniques. The hybrid threat may conduct a conventional military attack while simultaneously creating economic instability, fostering lack of trust in existing governance, attacking information networks, and conducting a propaganda campaign, perhaps while causing a humanitarian crisis.

1-69. Commanders facing a hybrid threat will have difficulty identifying and responding to specific challenges. If they faced them individually, U.S. forces could readily isolate and defeat each aspect of the hybrid threat. However, because hybrid threat actors integrate these capabilities across the operational area, they can continue to shift effort and emphasis to make all U.S. choices seem poor ones. Enemies can learn and adapt quickly, often unrestricted by rules or bureaucracy. The hybrid threat's continually shifting efforts may cause haphazard and incomplete change, but such rapid adaptation is difficult to counter. Ultimately, success goes to those who can act, react, and adapt their tactics quickly and creatively.

INFORMATION WARFARE

1-70. Information warfare refers to a threat's use of information activities, such as cyberspace attack and EW, to gain an advantage in the information environment. The threat construct of information warfare merges the disciplines of EW, deception, lethal fires, information protection, perception management, and cyberspace operations into a mutually supporting, integrated capability. Threat information warfare consists of—

- **EW**. Measures conducted to control or deny an enemy's use of the electromagnetic spectrum, while ensuring its use by the hybrid threat.
- **Deception**. Measures designed to mislead an enemy by manipulation, distortion, or falsification of information to induce the enemy to act in a manner prejudicial to their interests.
- **Physical destruction**. Measures to destroy critical components of communications infrastructure.

- **Protection and security measures**. Measures to protect the hybrid threat's information infrastructure and to deny protected information to other actors.
- **Perception management**. Information, misinformation, disinformation, and propaganda.
- **Information attack**. Attacks against the information resident on or transiting communications and information systems, rather than the systems themselves. Information attacks focus exclusively on the manipulation or degradation of the information to affect the information environment.
- **Computer warfare**. Measures ranging from unauthorized access (hacking) of information systems for intelligence collection purposes to the insertion of destructive viruses and deceptive information into enemy computer systems.

1-71. Because these elements share some of the same functions, means, and targets, the enemy or adversary can formulate and execute a single, integrated information warfare plan. Despite the name information warfare, adversaries continuously conduct these activities at every level of warfare across the competition continuum to set favorable conditions, protect their self-interests, and influence public opinion in an operational area.

1-72. Some threat information warfare capabilities, such as cyberspace attack and perception management, can reach far beyond the immediate operational area. An enemy or adversary may perform strategic information warfare activities to create effects globally, including attacks on critical U.S. infrastructure, military deception, and perception management campaigns to influence public support. Refer to FM 3-53 for more information about military deception and perception management.

1-73. An enemy or adversary may also undertake tactical actions to achieve information warfare objectives, rather than purely military ones. To some extent, managing, controlling, and disseminating information have always been critical to tactical success. This is especially true given the advances in information technology and U.S. reliance on network capabilities.

1-74. Adversaries recognize the advantages information warfare activities can provide their tactical commanders. Therefore, they strive to integrate information warfare planning and activities in all tactical missions and battles. Information warfare activities may degrade or deny U.S. communications and blur or manipulate the common operational picture. Information warfare may also help an enemy dictate the tempo of combat. By combining perception management, military deception, and EW, the enemy may be able to effectively slow or control the pace of battle. Traditional EW activities, such as jamming, also contribute to the tactical application of information warfare by challenging U.S. attempts to establish information advantage. Information advantage is the superior position or condition derived from the ability to securely access, share, and collaborate via trusted information while exploiting or denying an adversary's ability to do the same.

1-75. Threat information warfare also supports tactical counterreconnaissance. Threat actors constantly seek to attack, degrade, or manipulate U.S. intelligence, surveillance, and reconnaissance capabilities. Each U.S. and allied target acquisition system and sensor is a potential target.

1-76. Because threat actors integrate their information warfare capabilities, a coordinated and synchronized response is essential. The countermeasures to defend against these capabilities are a combination of signal, cyberspace operations, electronic protection, space, and other information-related capabilities, along with intelligence and operations security support. Close collaboration between these elements ensures a more effective response. Refer to TC 7-100 for more information about hybrid threat and information warfare.

THREAT ACTIVITIES IN CYBERSPACE

1-77. Threat actors can exploit system vulnerabilities and cause a loss of confidentiality, integrity, or availability of communications networks. Protecting the information on the Army network from internal and external threats is essential to maintaining freedom of action in cyberspace.

1-78. Threat actors include adversaries and enemies. The difference between them is that an adversary is potentially hostile, while an enemy is demonstrably hostile. This distinction is clear in the physical domains, but less so in cyberspace. An adversary may well take hostile actions against U.S. interests in cyberspace

without becoming an enemy that U.S. forces might engage in the physical domains. For this discussion, threat actors encompass both adversaries and enemies.

1-79. DOD networks and information systems face continuous risk from a variety of threat actors. Every day, DOD networks come under attack by threat actors including—

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

1-80. These threat actors use many methods to disrupt, degrade, destroy, exploit, alter, or otherwise adversely affect the Army's use of cyberspace. Elements of the network reside across the physical domains, with different methods of communicating and varying levels of interconnectivity and isolation. Threat actors may seek to exploit any network node, communications link, or the data residing in or traversing the nodes and links. Connecting critical infrastructure to the network exposes it to the risk of cyberspace attack.

1-81. Cyberspace allows threat actors to operate anonymously or to obscure their identity and location. This allows threat actors to pose as friendly actors and deceive individuals into divulging sensitive information or circumventing security measures—likely without realizing they have done so—through social engineering or phishing. Threat actors can attack Army systems, networks, and information assets by manipulating unsecured systems.

1-82. The same gateways that facilitate information exchange and allow legitimate outside users to access the network present attack vectors threat actors attempt to exploit. Threat actors often use the same commercial networks as noncombatant civilian populations, complicating cyberspace attack attribution and response.

Note. Social engineering uses techniques that rely on weakness in human nature rather than software. The goal is to deceive people into revealing passwords and other information that compromise the security of automated information systems and networks.

1-83. The broad range of threat actors in cyberspace increases the complexity in securing the Army network. The enduring nature of threat activities in cyberspace causes U.S. forces to expend considerable resources and effort securing DOD networks. Network-enabled operations are a force multiplier and a traditional strength of U.S. forces. However, network-enabled operations also create significant vulnerabilities. The extent to which U.S. forces rely on networked capabilities presents broad cyberspace and electromagnetic spectrum attack surfaces.

1-84. Failing to protect even one system can create a foothold into the network and place sensitive data, U.S. operations, and lives at risk. Even when cyberspace defenders discover and stop an attack, they might not be able to attribute it to a particular source. Following cybersecurity best practices, defending the network, and adhering to operations security guidelines help protect DOD networks and data.

1-85. Threat actors may undertake intelligence gathering within the Department of Defense information network (DODIN), either to support their operations or to counter U.S. operations. Exploitation reveals information resident on, or transiting through, a system. Threat intelligence activities can compromise sensitive operational information.

1-86. Trusted insiders with legitimate access to systems pose one of the most difficult threats to counter. Insiders are the most dangerous threat to operations security because they can readily access sensitive information.

1-87. A peer threat will systematically and continuously combine all available means to attack U.S. and allied network capabilities to create effects in the information environment. Peer threats will use deceptive tactics such as phishing attacks to gain access to Army networks for follow-on cyberspace operations.

1-88. Commanders must recognize the proliferation of threat cyberspace capabilities and their impact on operations. Threat activities in cyberspace can disrupt friendly information systems and degrade joint command and control. Threat operations in cyberspace are often less encumbered by treaty, law, and policy restrictions than those imposed on U.S. forces. This may allow enemies and adversaries an initial advantage in cyberspace. Signal support elements and staffs must maintain an effective cybersecurity program to secure the network against threat activities in cyberspace.

INSIDER THREAT

1-89. Insider threats present a significant risk to military operations. An *insider threat* is a person with placement and access who intentionally causes loss or degradation of resources or capabilities or compromises the ability of an organization to accomplish its mission through espionage, providing support to international terrorism, or the unauthorized release or disclosure of information about the plans and intentions of U.S. military forces (AR 381-12). Insider threats are hostile actors who intentionally compromise national security through deliberate actions. Insider threat should not be confused with operations security or cybersecurity risks, where sensitive operational information may be accidentally compromised and place U.S. operations or personnel at risk.

1-90. An insider threat does not necessarily need to be a military member or government employee. Third party vendors, contractors, and partners could pose a threat as well. The insider threat is especially dangerous because insider activity is generally the hardest to identify. Downloading or printing files to remove from secure areas may appear to be ordinary day-to-day activities. Similar to enemy cyberspace attacks, a trusted insider can steal sensitive data to undermine partner relationships or manipulate public opinion.

1-91. Past cases of insider threats have demonstrated that coworkers, associates, friends, and supervisors of those engaging in espionage or terrorist activity commonly overlook potential threat indicators. If these indicators had been reported and investigated, they might have minimized the damage to national security or saved the lives of U.S. personnel. The knowledge, awareness, and participation of all Department of the Army personnel in threat awareness and reporting is essential to the success of the Army's warfighting mission and in protecting the lives of Soldiers (AR 381-12).

SECTION II – FUNDAMENTAL PRINCIPLES OF SIGNAL SUPPORT

1-92. The network connects geographically separated forces for network-enabled operations. Because the Army conducts operations as part of a joint force, signal support requires joint interoperability in systems engineering, planning, deployment, and operation. Joint forces must be networked, linked, and synchronized in time and purpose so dispersed forces can communicate, maneuver, share information, collaborate, and share a common operational picture.

1-93. By integrating information from across the operational area, Army forces can maintain timely and relevant situational understanding. The integrated common operational picture allows commanders to manage operational risk and employ the right capabilities at the right place and time to achieve mission objectives. Making this possible requires signal Soldiers and leaders to apply the fundamental principles of—

- Operational focus.
- Interoperability.
- Agility.
- Trusted systems.
- Shared networks.
- Situational awareness.

OPERATIONAL FOCUS

1-94. Communications support should never be the limiting factor to the commander's ability to execute a mission. Signal staffs need to understand the commander's scheme of maneuver and intent and be able to articulate the capabilities and limitations of their communications systems to their commanders. This way, commanders can employ their signal capabilities to best support the operation.

1-95. Signal staffs must participate early in and throughout the operations process. Integration of the scheme of signal support into operations plans is essential to mission success. This integration requires signal planners at every echelon to participate as full partners in the military decision-making process. Signal planners participate throughout the planning process, so they can better understand the maneuver plan and anticipate changes in operational requirements. During course of action comparison, signal planners advise the commander and staff of capability shortfalls that will adversely affect a proposed course of action.

INTEROPERABILITY

1-96. Interoperability among unified action partners enables information advantage in joint and multinational operations. Sharing common technical standards and policies among joint mission partners allows a wide range of networking and information systems to interoperate as a joint network. Interoperability among systems and mission partners facilitates information exchange and speeds up decision making and implementation. Interoperability requires compatibility and standardization among communications and automated information systems. Planners must consider joint interoperability when formulating signal support plans.

COMPATIBILITY

1-97. Compatibility is the capability of two or more different items or components of equipment to function in the same system or environment without mutual interference. Electromagnetic compatibility, including frequency supportability, is a design consideration at the earliest conceptual stage and throughout the planning, design, development, testing, evaluation, and operational life cycle of all systems.

STANDARDIZATION

1-98. The need for standardization applies across the DOD, including the joint, Army, and other Services' networks. Operating all of these networks and enclaves under the same technical standards ensures interoperability among mission partners. Standardization enables collaboration with unified action partners and reduces duplication in research and development efforts.

AGILITY

1-99. Agile communications enable decentralized execution according to the commander's intent. Communications and networking capabilities must meet the commander's communications requirements and support decision-making processes. An agile network adapts to meets user needs in a continually changing operational environment. Agile networks have the capacity, flexibility, mobility, redundancy, reliability, scalability, and timeliness to meet commanders' requirements across the range of military operations. To support agile forces and operational concepts, the communications architecture should adapt to a wide range of missions without needing extensive reconfiguration.

CAPACITY

1-100. Signal staffs must plan communications and network capabilities to support all anticipated requirements in the operational area. High-level plans for the theater network must consider satellite bandwidth and spectrum availability to support growth as the theater network expands to meet increasing operational requirements.

FLEXIBILITY

1-101. Flexibility allows rapid integration at all levels of joint and Army automated information systems support. Flexibility allows signal elements to adapt to changing situations and dynamic operations with minimal disruption or delay. Flexibility is particularly important during contingency operations.

MOBILITY

1-102. Commanders at all levels must have network systems that are as mobile as the forces, elements, or organizations they support, without degraded information quality or flow. The network should provide an operational advantage and not a burden while enhancing the speed and agility of warfighting formations.

REDUNDANCY

1-103. Redundancy provides multiple transmission paths, backups, self-healing strategies, and data replication. Redundancy enables quick recovery if portions of the network or the data that it transports are destroyed, rendered inoperative, or degraded. Signal elements implement redundancy through—

- Communications in depth—using alternative communications means for connectivity in a degraded environment.
- PACE plans.

RELIABILITY

1-104. Reliability ensures networks are available when needed and perform as intended. Use of systems and networks with low failure rates, error correction techniques, and self-healing network architecture enhances the reliability of communications support.

SCALABILITY

1-105. Signal forces must provide a network that is tailorable to adapt, based on phases of an operation, to enable command and control at home station, en route, and in deployed environments. Deployed environments include training, exercises, theater security cooperation, initial entry, and maneuver. Deployed environments may involve minimal to robust force packages. Signal elements must be able to adjust the network to provide the right services at the point of need, under all conditions as the size of the supported deployed forces increases or decreases.

TIMELINESS

1-106. Timeliness ensures that the processing and transmission time for warning, critical intelligence, and operation order execution information is as short as practicable. As weapon systems technology shortens the time between warning and attack, information management processes must reduce the lag between information collection and dissemination.

1-107. Signal elements perform information management in support of the unit's knowledge management plan to ensure commanders and their staffs receive the information they need, when they need it, to support planning and decision making. As the network expands or network nodes displace to meet mission requirements, signal elements ensure timely network support through—

- Priorities of work.
- Priorities of service.
- Quality of service management.

TRUSTED SYSTEMS

1-108. Commanders and system users need to be able to trust the confidentiality, integrity, and availability of automated information systems. Trusted networks must be transparent to users, protect the information and services on the network, and provide users with confidence in the validity of the information the network delivers. Trusted networks must be protected, survivable, and sustainable.

PROTECTION

1-109. Protected communications systems and networks enable joint command and control in a contested environment. As such, they present high-value targets to the enemy. Cybersecurity and communications security (COMSEC) secure DOD networks and the information they carry. Cybersecurity establishes the

baseline security of the network. COMSEC secures network transport media and classified terminal devices. Signal elements protect the network through—

- Cybersecurity.
- COMSEC.
- Electronic counter-countermeasures (anti-jamming techniques).

SURVIVABILITY

1-110. Survivable networks result from techniques such as dispersal of key facilities, redundant communications nodes, or a combination of techniques necessary for the physical and electrical protection of networks and critical infrastructure. While it is not practical or economically feasible to make all networks or elements of a system equally survivable, the networks and systems that enable command and control need protection commensurate with the survivability requirements of the associated command post. Since the Army network is a key command and control enabler, enemies consider it a key target for lethal and nonlethal fires.

SUSTAINABILITY

1-111. Sustainable networks provide support during any type of operation, regardless of its duration. This requires the economical design and employment of networks without sacrificing operational capability or survivability. Examples that might improve system sustainability include—

- Consolidating functionality of similar facilities.
- Adherence to joint-approved architectures.
- Integrating special purpose and dedicated networks, when possible, into the joint portion of the DOD network.
- Maximum use of DOD-wide common user services.
- Judicious use of commercial services to augment military capabilities.

SHARED NETWORKS

1-112. Shared networks and services allow the mutual use of information services and communications capabilities among unified action partners at all echelons. Shared networks enable collaboration, rapid dissemination of intelligence and information, and the ability to project decisions based on common situational understanding. Signal elements provide shared networking capabilities by implementing—

- DOD-wide common standards—common cybersecurity policies and system configurations to enhance interoperability.
- Cybersecurity reciprocity—sharing security authorization packages and agreeing to accept other Services' test and assessment results and authorization.
- Mission partner environment—secure networking environment for multinational collaboration.

NETWORK SITUATIONAL AWARENESS

1-113. Comprehensive network situational awareness allows commanders and their staffs to receive, correlate, and display an accurate representation of systems and networks. A clear visual representation of the network allows near real-time assessment of operational impacts and helps staffs identify key terrain in cyberspace.

1-114. Observation of the intensity of network activity, traffic load, and data throughput yields network situational understanding to enable dynamic rerouting of priority traffic and services and may provide indications of cyberspace or electronic attack. Situational awareness allows commanders and signal elements to—

- Monitor, protect, and prioritize their network assets.
- Assess the operational impact of network disruptions.
- Respond to network outages or attacks.

- Dynamically reallocate network traffic.

OBJECTIVES OF SIGNAL SUPPORT

1-115. Signal elements and capabilities exist to meet commanders' information requirements and enable control of forces. The Army network extends from the lowest tactical echelons to the highest levels of command. As a warfighting platform, the network enables commanders to integrate combined arms and all elements of combat power. Signal capabilities support command and control and enable strategic responsiveness, ultimately leading to a marked information advantage in the operational area.

SUPPORT TO COMMAND AND CONTROL

1-116. The fundamental principle of operational focus supports the commander's exercise of command and control. Signal elements can adapt the network based on the operational phase or tactical situation to meet the commander's information requirements at the home station, en route, or while deployed. The fundamental principle of scalability enables signal leaders to tailor signal support to the purpose and scope of the deployment. Supporting signal elements adjust the network to provide appropriate services at the point of need, under all conditions

STRATEGIC RESPONSIVENESS

1-117. Strategic responsiveness requires Army forces to react quickly to changes in the operational environment. The fundamental principles of operational focus, interoperability, agility, and shared networks allow signal support to rapidly adapt and scale the network to support any mission or situation. Joint and Army networks provide worldwide strategic voice and data capabilities and prepositioned connection points to extend services to expeditionary forces. Expeditionary signal capabilities provide the same types of services used at the home station, whenever and wherever rapidly-deployable forces are needed.

1-118. Signal network capabilities enable leaders to receive, process, and disseminate information globally. Strategic responsiveness allows leaders to see and understand the significance of situations around the world and then make and disseminate decisions, resulting in action. These network capabilities support coordinated planning, preparation, execution, and synchronization with unified action partners.

INFORMATION ADVANTAGE

1-119. Signal elements who successfully apply all of the fundamental principles of signal support provide their commander an information advantage. The Army network allows commanders and staffs to access timely, protected information when and where they need it to meet their critical information requirements. Access to information results in an information advantage and enables decision making, leadership, and combat power. Information advantage is a key to gaining and retaining the initiative and consolidating gains in the operational environment. Signal support enables information advantage by providing communications and information technology systems, information management processes, and operational procedures that give commanders the ability to—

- Focus on building an accurate, current, common operational picture.
- Enhance and share knowledge, understanding, and visualization of the operational environment.
- Improve and sustain the quality and speed of collaboration and decision making.

CORE COMPETENCIES OF THE SIGNAL CORPS

1-120. Signal Soldiers and units apply the fundamental principles of signal support by executing the core competencies and essential capability of the Signal Corps. The core competencies are—

- DODIN operations.
- Network transport and information services.
- Spectrum management operations.
- Visual information and combat camera.

1-121. COMSEC, while not a core competency, is an essential capability of signal support to implement trusted systems. Together, the core competencies and essential capability enable commanders' exercise of command and control and integration of the other warfighting functions. Chapter 2 contains a more detailed discussion of the core competencies and essential capability of the Signal Corps.

SECTION III – SIGNAL IN ARMY OPERATIONS

SUPPORT TO JOINT OPERATIONS

1-122. The Army is interdependent with the joint force and serves as the foundation on which the joint force conducts land operations. The Army conducts operations to gain, sustain, and exploit control over land to deny its use to an enemy. It does this with combined arms formations with the mobility, firepower, and protection to defeat an enemy and establish control over land, resources, and populations. Army capabilities enable joint force success across multiple domains, and in the information environment. The Army provides key enabling capabilities to the joint force, including communications, intelligence, protection, and sustainment support.

1-123. A secure, robust, and reliable communications system gives the joint force commander the means to assimilate information and to exercise authority and direct forces over large geographic areas and a wide range of conditions. A communications system that provides connectivity throughout the operational area from the strategic to tactical levels is vital to plan, conduct, sustain operations, and enable information superiority (JP 6-0). Joint commanders use the network to exercise command and control and integrate the joint force components.

1-124. Army contributions to joint command and control include establishing, maintaining, and defending the communications and network architecture to support Army and joint forces in the theater. The network provides connectivity between Army forces and unified action partners in the joint operations area.

1-125. Army communications planners must include joint interoperability in their plans. Differences in policies, technologies, levels of capabilities, and resources when integrating communications support between joint and multinational forces create challenges that cannot be mitigated without in-depth planning at all levels. As an example, when integrating with joint mission partners, Army network planners must align their information sharing, COMSEC, technical engineering, and interconnection policies and procedures with those established by the communications system directorate of a joint staff (J-6). Considering interoperability requirements as early as possible in the planning process mitigates the added complexity of joint communications planning.

1-126. The DODIN-A can adapt, and the network main effort shifts, as the theater matures and forces transition between phases of an operation. DODIN operations control authorities and responsibilities shift as an operation matures and units arrive in the affected theater. Refer to ATP 6-02.71 for details on the transfer of DODIN operations authorities across the operational phases.

ARMY STRATEGIC ROLES

1-127. The Army accomplishes its mission by supporting the joint force in four strategic roles: shape operational environments, prevent conflict, conduct large-scale ground combat, and consolidate gains (FM 3-0). Strategic roles are not tasks assigned to subordinate units, but broad goals of an Army force. The Army conducts tactical tasks to accomplish each of its strategic roles to varying extents across each phase of an operation. Refer to FM 3-0 for more information about the Army's strategic roles.

SHAPE OPERATIONAL ENVIRONMENTS

1-128. Army operations to shape help dissuade adversary activities designed to achieve regional goals short of military conflict. As part of operations to shape, the Army provides trained and ready forces to geographic combatant commanders in support of their theater campaign plan. The theater army and subordinate Army forces assist the geographic combatant commander in building partner capacity and capability and promoting

stability across the area of responsibility (FM 3-0). Army operations to shape take place continuously before, during, and after a joint operation within a specific operational area.

1-129. Signal forces may contribute to shaping by conducting security cooperation activities to help build partner nation capacity, capabilities, and interoperability. Forward deployed strategic signal units provide peacetime and contingency access to the DODIN-A in theater. See chapter 3 for more information about signal support to operations to shape.

PREVENT CONFLICT

1-130. Army operations to prevent include all activities to deter an adversary's undesirable actions. These operations are an extension of operations to shape designed to prevent adversary opportunities to further exploit positions of relative advantage by raising the potential costs to adversaries of continuing activities that threaten U.S. interests. Prevent activities are generally weighted toward actions to protect friendly forces, assets, and partners, and to indicate U.S. intent to execute subsequent phases of a planned operation (FM 3-0).

1-131. Signal activities during operations to prevent include—predeployment activities, initial entry, and development of theater infrastructure. Theater army planners develop contingency communications plans to support the geographic combatant commander's concept of operations. See chapter 3 for more information about signal support to operations to prevent.

CONDUCT LARGE-SCALE GROUND COMBAT

1-132. During large-scale combat operations, Army forces focus on the defeat and destruction of enemy ground forces as part of the joint team. Army forces close with and destroy enemy forces in any terrain, exploit success, and break their opponent' s will to resist. Army forces attack, defend, conduct stability tasks, and consolidate gains to attain national objectives (FM 3-0)

1-133. During large-scale ground combat, organic signal elements at corps and below support command post operations for planning and support. Maneuver elements rely mainly on single-channel radios and friendly force tracking capabilities. See chapter 4 for more information about signal support to large-scale combat operations.

CONSOLIDATE GAINS

1-134. Consolidation of gains is an integral and continuous part of armed conflict, and it is necessary for achieving success across the range of military operations (FM 3-0). Consolidation of gains is deliberate and takes place during all phases of an operation. Consolidation of gains becomes the primary focus of Army forces at the conclusion of large-scale combat operations. Signal activities to consolidate gains may include transitioning to commercial communications infrastructure. See chapter 5 for more information about signal support to the consolidation of gains.

THE ARMY OPERATIONAL CONCEPT

1-135. Army forces contribute to the joint mission through the conduct of unified land operations as part of a joint and multinational force. *Unified land operations* is the simultaneous execution of offense, defense, stability, and defense support of civil authorities across multiple domains to shape operational environments, prevent conflict, prevail in large-scale ground combat, and consolidate gains as part of unified action (ADP 3-0).

1-136. Commanders conducting network-enabled operations need secure communications and automated information systems that operate reliably and adapt to changing requirements, transparent to users. These systems support U.S. and multinational forces at every level of command. The DOD network that supports network-enabled operations is the DODIN. 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). Signal Soldiers and formations support Army operations with secure network connectivity and information services at all echelons.

SUPPORT TO COMMAND AND CONTROL

1-137. Combined arms maneuver is impossible unless commanders have the expertise and communications to synchronize Army and joint combat power. The science of control—regulating, monitoring, and directing unit actions—requires sophisticated and rugged information systems, along with a well-trained staff to employ them. Even knowledgeable and charismatic commanders cannot control everything beyond their immediate surroundings without the supporting personnel, networks, information systems, processes and procedures, and facilities and equipment (ADP 1).

1-138. The command and control system enhances the commander's ability to conduct operations. Commanders arrange the four components of the command and control system (see introductory figure-2) to—

- Support decision making.
- Collect, create, and maintain relevant information and prepare knowledge products to support situational understanding and visualization.
- Prepare and communicate directives.
- Establish the means to communicate, collaborate, and facilitate the functioning of teams.

1-139. Signal Soldiers and units provide the network and automated information systems to support the commander's exercise of command and control. Networks enable successful operations. Commanders determine their information requirements and focus their staffs and organizations on using networks to meet these requirements. These capabilities relieve staffs from handling routine data, and enable extensive information sharing, collaborative planning, execution, and assessment that promote shared understanding (ADP 6-0). Networks also assist commanders in projecting their decisions across the force. The Army's network is the DODIN-A. The DODIN-A enables the warfighting functions of command and control, fires, intelligence, movement and maneuver, protection, and sustainment, and provides the commander and staff the information they need to support sound decision making.

1-140. Signal support enables the commander to exercise command and control and to integrate the other warfighting functions (see introductory figure-1 on page viii). The DODIN-A and automated information systems enhance the ability to plan and coordinate operations across staff sections, cells, command posts, and echelons. Signal Soldiers—

- Install, operate, maintain, and secure the DODIN-A (DODIN operations and COMSEC).
- Formulate signal support plans as part of the military decision-making process.
- Conduct information management.

1-141. As a warfighting platform, the DODIN-A enables commanders to integrate joint combined arms and all elements of combat power. Command post personnel, information systems, and equipment must be able to support continuous operations while in communication with their higher echelon, subordinate, supporting, supported, and adjacent units (FM 3-0). The DODIN-A connects command posts, weapon platforms, dismounted Soldiers, and sensors, enabling the command and control system to—

- Support leaders' ability to understand, visualize, and describe the operational environment, problems, and approaches to solving them (situational understanding).
- Support commanders' ability to make decisions and direct action toward a desired end state.
- Assess understanding of—
  - The problem.
  - Adequacy of the operational approach and subsequent plans.
  - Level of progress.

1-142. Adversaries and enemies will target command and control systems. Units must adapt their command and control systems to the realities of fighting peer threats. Conditions in large-scale combat operations require the smallest possible physical footprint and electronic signature and the highest possible level of

agility. Close coordination between the G-6 (S-6) and the EW section can help identify and minimize the command posts' electronic signature.

1-143. The DODIN-A supports global, distributed command and control and enables the Army to fight and win in a congested and contested operational environment. The DODIN-A integrates information services and capabilities at all strategic, operational, and tactical echelons and enables all warfighting functions.

1-144. Signal elements can adapt the network based on the operational phase or tactical situation to provide command and control capabilities in support of training and exercise, theater security cooperation, forcible entry, large-scale combat operations, and stability activities. The purpose and scope of the deployment determine the size and capability of the forces required. Supporting signal elements adjust the network to provide appropriate services at the point of need, under all conditions.

1-145. Home station mission command centers enable units to conduct split-based operations. Controlling an operation from the home station and deploying a smaller, forward-deployed command post reduces the deployed footprint and operational risk. Utilizing the home station mission command center, the division can deploy a smaller, tailored command post for initial entry operations, conduct major planning at the home station, and use reachback to the home station.

SUPPORT TO OTHER WARFIGHTING FUNCTIONS

1-146. Signal Soldiers and units support all warfighting functions by installing, operating, and securing the DODIN-A to provide connectivity to critical Defense Information Systems Network (DISN) services. These services include the Defense Switched Network, Defense Red Switched Network, Organizational Messaging Service, video teleconferencing, telemedicine services, SECRET Internet Protocol Router Network (SIPRNET), Non-Classified Internet Protocol Router Network (NIPRNET), Joint Worldwide Intelligence Communications System, and mission partner environment.

1-147. Reliable, secure communications and information services enable commanders to exercise command and control and to integrate the other warfighting functions. The warfighting functions are mutually supportive. The DODIN-A connects people to enable resource and information sharing and collaboration. As information passes between elements, the network enables coordination to support the commander's intent. Integration of the warfighting functions relies on the network for information sharing.

1-148. Information and communications requirements change with the operational and mission variables. Signal elements can adapt the network to continue supporting, and enabling the integration of, all warfighting functions. The network can expand or contract to meet the commander's changing information requirements. As forces enter or leave an operational area, signal elements scale the theater network to meet mission requirements.

1-149. Network changes take deliberate planning and sometimes require additional resources. Considering network requirements early in the planning process ensures the network can fully support the unit's communications requirements. Identifying communications gaps during early planning allows commanders to request augmentation, as necessary.

MULTINATIONAL INTEROPERABILITY

1-150. Army forces integrate, both operationally and organizationally, with joint, interorganizational, and multinational mission partners. The traditional model of multinational operations, where each mission partner operated in a separate area of operations and maintained a separate national classified network interferes with information sharing and unity of effort. A tailored mission network in which unified action partners share classified information and operate as equals enhances interoperability and facilitates multinational cooperation.

1-151. The Defense Information Systems Agency maintains configuration standards and joining instructions for mission partner environment. By adopting common standards and configurations, unified action partners can share classified information freely without compromising the security of the information. Mission partner environment increases battlefield effectiveness by enabling unity of effort among diverse mission partners.

STRATEGIC AND OPERATIONAL REACH

1-152. Strategic and operational reach enable Army forces to deploy rapidly, fight on arrival, and conduct extended campaigns as part of a joint and multinational force. Doing so requires proficiency at force projection, protection, and sustainment. Soldiers require an expeditionary mindset to prepare them for short notice deployments into uncertain, often austere, and lethal environments.

1-153. Strategic reach provides the capability to operate against threats operating anywhere in the world. The distance across which the United States can project decisive military power is its strategic reach (FM 3-0).

1-154. *Operational reach* is the distance and duration across which a force can successfully employ military capabilities (JP 3-0). Extending operational reach is a major concern for commanders throughout an operation. The limit of a unit's operational reach is its culminating point. Signal support using beyond line of sight satellite communications capabilities extends operational reach by increasing the geographic area a commander can effectively control.

OPERATIONAL MOVEMENT AND MANEUVER

1-155. Operational movement and maneuver combines global force projection with maneuver against an operationally significant objective. Successful operational movement and maneuver allows a unit to—

- Secure and defend a lodgment.
- Develop support infrastructure and base camps.
- Receive, stage, and build up forces.

1-156. Signal support to operational movement and maneuver combines operational science and art to ensure the right capabilities are available to support Army commanders, staffs, and units at the right time and place. The science of signal support is the technical aspects of communications and the ability to properly employ the Army's wide variety of communications capabilities. The G-6 (S-6) must understand the operation plan and articulate the capabilities and limitations of the unit's communications assets. The scheme of signal support effectively distributes capabilities across the organization and employs the network in a manner that ensures the commander's ability to exercise command and control at any time and place on the battlefield.

EXPEDITIONARY CAPABILITY

1-157. The Army requires expeditionary forces with the endurance to prevail in protracted conflict against determined enemies. Expeditionary capability requires deploying the right mix of Army forces to the right place at the right time to achieve the desired mission objectives.

1-158. Expeditionary signal systems and formations enable commanders' exercise of command and control in a constrained environment, whether they are restricted to single-channel radios or are operating with full DODIN-A capabilities. The tactical portion of the DODIN-A can scale up or down to meet changing operational needs. The signal staff determines the smallest, least complex system available, and the minimum staffing necessary to meet the expeditionary mission requirement. Signal staffs determine whether to deploy servers forward, utilize reachback to the home station, or rely on strategic enterprise services to support an expeditionary mission.

FORCE PROJECTION

1-159. Force projection is the military component of power projection. Seizing the initiative generally requires force projection. Force projection is a race between friendly and enemy forces. The side that most rapidly builds combat power can seize the initiative. During force projection, the ability to scale communications packages up or down to meet mission requirements gives commanders flexibility when tailoring force projection packages.

ENTRY OPERATIONS

1-160. The entry of Army and joint forces into a joint operations area or theater of operations may be unopposed or opposed (FM 3-0). Being part of an expeditionary force means units deploy on short notice to austere locations. Maintaining communications en route to the operational area allows units to refine their plans while in transit and arrive in the area of operations with current intelligence estimates ready to immediately conduct combat operations.

1-161. Attaining operational reach often requires gaining and maintaining operational access in the face of enemy antiaccess and area denial capabilities and actions. Commanders conduct forcible entry operations to seize and hold a military lodgment in the face of armed opposition.

Early and Initial Entry

1-162. During the initial phases of an operation, units may not be able to deploy heavy wideband satellite communications trailers and nodal systems. Signal leaders need to deploy their communications capabilities in phases and build network capacity over time. Initial entry operations may be supported solely with single-channel, push-to-talk radios. Commercial cellular networks and devices may augment single-channel radios until adequate signal support becomes available in the operational area, but commanders' risk decisions must account for peer threat capabilities to exploit cellular networks for location information and intelligence collection. Expeditionary units must be prepared to operate with limited communications capabilities in austere locations. Signal planners must effectively deploy the solutions that maximize capabilities within the limitations of the situation or environment.

Forcible Entry

1-163. *Forcible entry* is seizing and holding of a military lodgment in the face of armed opposition or forcing access into a denied area to allow movement and maneuver to accomplish the mission (JP 3-18). Army forces, as part of a joint force, must be capable of deploying and fighting to gain access to geographic areas controlled by forces hostile to U.S. national interests to be credible both as a deterrent and as a viable military option for policy enforcement (FM 3-0).

1-164. Forcible entry operations are inherently complex and always joint. Often only hours separate the alert from the deployment. The demands of simultaneous deployment and employment create a distinct set of dynamics. Operations are carefully planned and rehearsed in training areas and marshalling areas. Personnel and equipment are configured for employment upon arrival without reception, staging, onward movement, and integration (FM 3-0).

1-165. Joint interoperability of signal systems enables units to conduct forcible entry operations with joint and multinational partners. Interoperable communications allow mission partners to synchronize their efforts and share situational awareness to prevent friendly fire.

1-166. Because communications systems must be built-up at the objective area, some aspects of communications support are unique in forcible entry operations. Communications requirements for joint forcible entry operations vary with the mission, size, composition, and geographic location of the joint force and its senior headquarters. Significant requirements to consider for forcible entry operations are the use of intermediate staging bases, en route mission planning, and intelligence sharing.

1-167. Ground commanders in airlift aircraft may communicate with the chain of command over the Army secure en route communications package. Normally, the airlift mission commander and the airborne task force commander are in the same aircraft. The senior ground commander can advise embarked ground commanders of changes in the ground tactical situation or to the air movement plan (JP 3-18).

1-168. Forces initially deploy with limited communications capabilities—primarily single-channel radios and narrowband (single-channel) satellite communications. As additional units enter the operational area, the deployed network becomes more robust to support greater troop strength and associated command posts. Refer to JP 3-18 for more information about forcible entry operations.

This page intentionally left blank.

Chapter 2

Signal Support by Army Echelon, Core Competencies, Training, and the Army Network

This chapter discusses Army signal capabilities by echelon, the core competencies of the Signal Corps, signal collective training in units, and the Department of Defense information network-Army.

SECTION I – SIGNAL SUPPORT BY ECHELON

2-1. Deployable signal elements support the Army's operational needs, whether they are pooled assets or organic to a maneuver or support unit. Unique signal units provide strategic communications infrastructure or perform specialized missions and functions.

CORPS AND BELOW ORGANIZATIONS WITH ORGANIC SIGNAL ASSETS

2-2. Combat and combined arms units at echelons corps and below have organic signal capabilities to conduct their standard missions without requiring outside signal support. However, augmentation of communications capabilities is required for most enabler units, and if the unit's operational reach expands beyond the capabilities of their organic systems.

2-3. A brigade combat team may have company- or platoon-sized elements operating beyond the reach of single-channel radios, or that require more robust network connectivity and services than those provided by the brigade's organic signal capabilities. This becomes a downward-reinforcing mission of the theater tactical signal brigade and expeditionary signal battalion. Refer to ATP 6-02.60 for more information about the organic network communications capabilities of corps and below units.

CORPS

2-4. The corps is the principal headquarters for applying landpower as a component of a campaign (FM 3-94). The corps integrates landpower into campaigns and serves as the link between the operational and tactical levels of war.

2-5. The organic signal capabilities of the corps support its main and tactical command posts. When the corps serves as a joint task force headquarters, as a joint or multinational land component command, or as a tactical headquarters commanding multiple divisions, it may require augmentation from other Services or pooled signal assets from the theater tactical signal brigade.

Corps G-6

2-6. The G-6 is the principal staff officer who advises the commander on all matters related to communications in the corps. The G-6 advises the corps commander, staff, and subordinate commanders on technical and training issues related to network and information service integration. During split-based operations, the G-6 usually aligns with the tactical command post, while the deputy G-6 remains with the main command post. The corps G-6 coordinates with G-3 to direct the actions and movements of signal elements to support operations through the orders process.

2-7. The G-6 coordinates with higher, adjacent, and subordinate echelons to ensure adequate network support. See appendix B for more information about collaboration with higher, adjacent, and subordinate signal elements.

2-8. The G-6 controls DODIN operations in the corps area of operations through the network operations and security center. The corps network operations and security center establishes the corps portion of the DODIN-A. The network operations and security center provides operational and technical support to subordinate signal elements through technical channels. *Technical channels* are the chain of authority for ensuring the execution of clearly delineated technical tasks, functions, and capabilities to meet the dynamic requirements of Department of Defense information network operations (ATP 6-02.71). The network operations and security center monitors the health of the network and directs fault, configuration, accounting, performance, and security management. When operating as part of a joint task force headquarters, the corps network operations and security center forms the core of the joint network operations control center, with augmentation.

Note. Signal personnel often incorrectly refer to a 'network operations chain of command.' The correct term to describe the chain of authority for the conduct of DODIN operations is technical channels.

2-9. DODIN operations technical channels align with the operational chain of command to maintain unity of command and unity of effort. This allows commanders to manage the network as a warfighting platform and align available communications and network support capabilities to their highest mission priorities during each phase of an operation. Battalions configure their systems to report status information to the brigade network operations and security center. Each subsequent network operations and security center reports status to the next higher level of command. The regional cyber center monitors status of the theater network through the regional hub node on behalf of the theater army. Figure 2-1 depicts the DODIN operations technical channels at corps and below. Refer to ATP 6-02.71 for more information about DODIN operations monitoring and reporting.

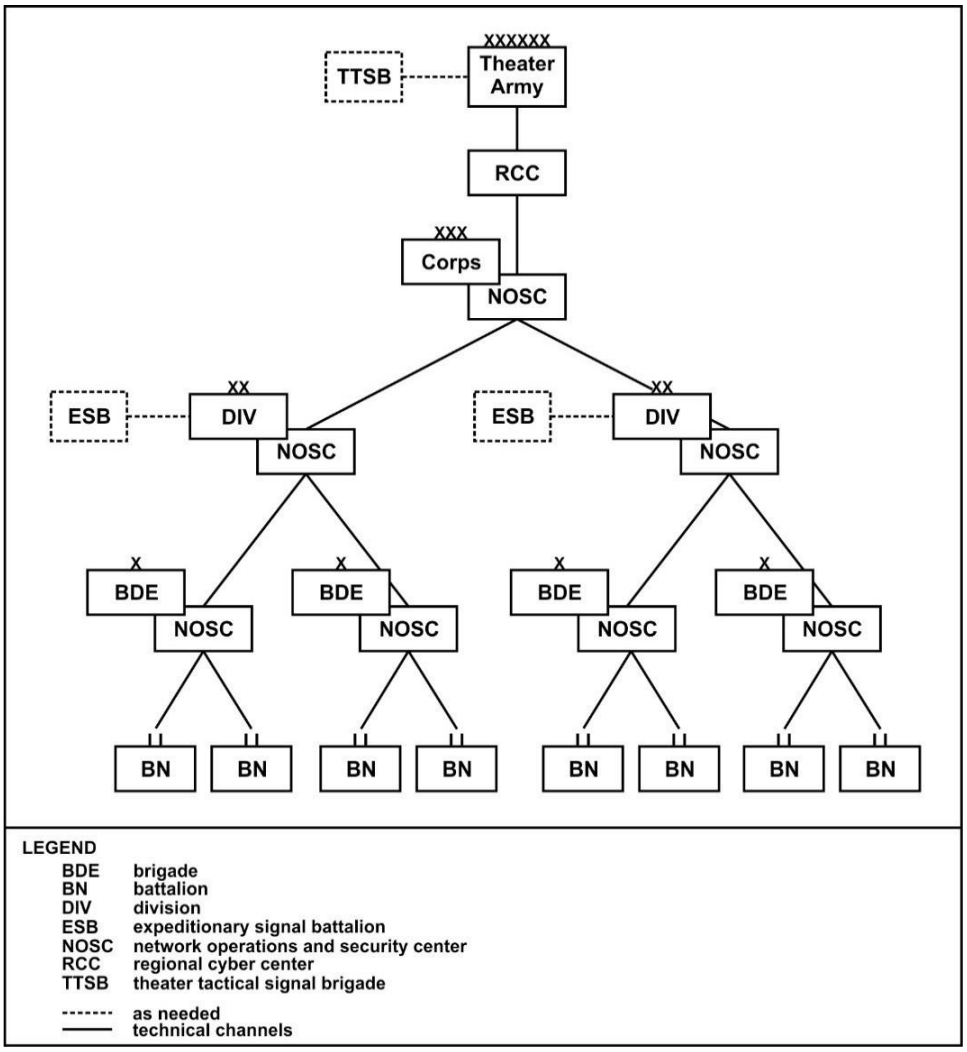


Figure 2-1. Department of Defense information network operations technical channels at corps and below

2-10. The corps G-6 integrates the corps network and automated information systems. The G-6 prepares the communications plan and exercises technical control over the signal portion of the corps signal, intelligence, and sustainment company in executing the plan. After initializing the local area networks, the G-6 establishes a 24-hour service desk to help with user issues and local area network connectivity in the command posts. The roles and responsibilities of the G-6 include—

- Developing the scheme of signal support to operation orders through the military decision-making process, including PACE plans for each phase of the operation.
- Assist the commander and G-3 in identifying user requirements by number and service type.
- DODIN operations planning.
- Satellite communications planning.
- Line of sight network planning.
- Tactical radio network planning.
- Spectrum management.
- COMSEC account management.
- Integrating mission command information systems in the corps network.

- Coordinating, planning, and directing integration of unified action partner networks (mission partner environment).
- Local area network management for the corps command posts.
- Service desk management.
- Helping collect and disseminate relevant input to the common operational picture.
- Supporting the cyberspace electromagnetic activities (CEMA) section, as required.
- Information dissemination management to ensure awareness of relevant, accurate information, automated access to newly discovered or recurring information, and timely information delivery to support decision making.
- Signal maintenance and logistical readiness oversight for communications-electronics equipment.

2-11. When the corps headquarters serves as a joint task force headquarters, the G-6 usually serves as the joint task force J-6. This mission requires augmentation from other Services or pooled Army tactical signal assets.

Corps Signal, Intelligence, and Sustainment Company

2-12. The signal portion of the corps signal, intelligence, and sustainment company operates under the technical control of the corps G-6. The company includes staffing for the G-6 section and elements to install, operate, maintain, and secure the corps headquarters' network transport, automated information systems, and networks. Refer to relevant intelligence and sustainment doctrine publications for more information on the company's intelligence and sustainment functions.

2-13. The corps signal, intelligence, and sustainment company provides communications and network support for the corps main and tactical command posts and the various companies in the corps headquarters and headquarters battalion. The signal portion of the company also provides—

- Wideband and protected satellite communications transport to connect with the DODIN-A.
- High-throughput line of sight transport to communicate between command posts.
- DISN services—SIPRNET, NIPRNET, Joint Worldwide Intelligence Communications System, voice, and video.
- Wire, cable, and fiber optic systems to support the corps command posts.
- Single-channel radio and narrowband (single-channel) tactical satellite retransmission for the corps and support elements.
- Global Broadcast Service capability to receive high bandwidth imagery, logistics data, and digital map information to support command and control.

Note. Employing a retransmission team remotely from established command posts or other units requires additional planning and resources for site defense, logistics, and emergency evacuation. Refer to ATP 6-02.53 for more information about retransmission planning.

DIVISION

2-14. The division is the Army's primary tactical warfighting headquarters. Its primary role is as a tactical headquarters commanding brigades in decisive action (FM 3-94). The division's organic signal capabilities support operations from traditional main and tactical command posts, as well as command and control on-the-move. The division's home station mission command center supports split-based operations. Although the division has organic signal capabilities, most enablers and other attached units require augmentation. As the division's operational reach expands, smaller units without organic signal capabilities require augmentation. This is a downward reinforcing mission of the theater tactical signal brigade.

Division G-6

2-15. The G-6 is the principal staff officer who advises the commander on all matters related to communications in the division. The G-6 advises the division commander, staff, and subordinate

commanders on technical and training issues related to network and information service integration. During split-based operations, the G-6 usually aligns with the tactical command post, while the deputy G-6 remains with the main command post. The division G-6 coordinates with the G-3 to direct the actions and movements of signal elements to support operations through the orders process.

2-16. The G-6 coordinates with higher, adjacent, and subordinate echelons to ensure adequate network support. The G-6 recommends network changes as needed to support the commander's intent. See appendix B for more information about signal planning and collaboration with higher, adjacent, and subordinate signal elements.

2-17. The division G-6 conducts DODIN operations in their area of operations through the division network operations and security center. The division network operations and security center establishes the division's portion of the DODIN-A. The network operations and security center provides guidance to subordinate signal elements through technical channels. The network operations and security center monitors the health of the network and directs fault, configuration, accounting, performance, and security management. When the division acts as a joint task force headquarters, the division network operations and security center forms the core of the joint network operations control center, with augmentation.

2-18. The division G-6 integrates the division's network and information systems. The G-6 prepares the communications plan and exercises technical control over the division signal company in executing the plan. After initializing the local area networks, the G-6 establishes a 24-hour service desk to help with user issues and local area network connectivity in the command posts. The roles and responsibilities of the G-6 include—

- Developing the scheme of signal support to operation orders through the military decision-making process, including PACE plans for each phase of the operation.
- Assist the commander and G-3 in identifying user requirements by number and service type.
- DODIN operations planning.
- Satellite communications planning.
- Managing satellite communications networks for the division and subordinate brigade combat teams.
- Line of sight network planning.
- Managing line of sight networks for the division and subordinate brigade combat teams.
- Tactical radio network planning.
- Spectrum management.
- COMSEC account management.
- Integrating mission command information systems in the division network.
- Coordinating, planning, and directing integration of unified action partner networks (mission partner environment).
- Local area network management for the division command posts.
- Service desk management.
- Helping collect and disseminate relevant input to the common operational picture.
- Supporting the CEMA section, as required.
- Information dissemination management to ensure awareness of relevant, accurate information, automated access to newly discovered or recurring information, and timely information delivery to support decision making.
- Signal maintenance and logistical readiness oversight for communications-electronics equipment.

2-19. When the division headquarters serves as a joint task force headquarters, the G-6 usually serves as the joint task force J-6. This mission requires augmentation from other Services or pooled signal assets.

Division Signal, Intelligence, and Sustainment Company

2-20. The signal portion of the division signal, intelligence, and sustainment company operates under the technical control of the division G-6. The company installs, operates, maintains, and secures the division's network transport, automated information systems, and networks and provides the G-6 staff. The division's organic signal capabilities support operations at-the-halt from the main and tactical command posts, and

command and control on-the-move. Refer to relevant intelligence and sustainment doctrine publications for more information on the company's intelligence and sustainment functions.

2-21. The signal portion of the division signal, intelligence, and sustainment company supports the division command posts and the various companies in the division headquarters and headquarters battalion. The company also provides—

- Wideband and protected satellite communications transport to connect with the DODIN-A.
- Gateway access to the DODIN-A through the tactical hub node, if regional hub node service is not available.
- High-throughput line of sight transport to communicate between fixed command posts.
- Line of sight and wideband satellite communications transport to support command and control on-the-move.
- DISN services—SIPRNET, NIPRNET, Joint Worldwide Intelligence Communications System, voice, and video.
- Single-channel radio and narrowband (single-channel) tactical satellite retransmission for the brigade and support elements.
- Wire, cable, and fiber optic systems to support the division command posts.
- Global Broadcast Service capability to receive high bandwidth imagery, logistics data, and digital map information to support command and control.

BRIGADE COMBAT TEAM

2-22. The brigade combat team provides the division, land component command, or joint task force with close combat capabilities. The brigade combat team's organic signal capabilities support operations at-the-halt from the main and tactical command posts. Active component infantry and Stryker brigade combat teams' signal capabilities also support command and control on-the-move.

Brigade Combat Team S-6

2-23. The S-6 is the principal staff officer who advises the commander on all matters related to communications in the brigade. The S-6 advises the brigade combat team commander, staff, and subordinate commanders on technical and training issues related to network and information service integration. The S-6 directs planning and coordination for DODIN operations, network transport and information services, and spectrum management operations for the brigade headquarters and subordinate units through the military decision-making process (see appendix B).

2-24. The S-6 collaborates with the higher headquarters J-6 or G-6, assigned or attached battalion S-6 staffs, and adjacent units to ensure effective communications throughout the brigade area of operations. The S-6 recommends network changes as needed to support the commander's intent. The brigade S-6 coordinates with the S-3 to direct the actions and movements of signal company elements to support operations through the orders process.

2-25. The S-6 conducts DODIN operations for the brigade and subordinate battalions through the brigade network operations and security center. The network operations and security center establishes the brigade's portion of the DODIN-A. The network operations and security center provides guidance to subordinate signal elements through technical channels. The network operations and security center monitors the health of the network and directs fault, configuration, accounting, performance, and security management.

2-26. The S-6 integrates the brigade's network and automated information systems. The S-6 prepares the communications plan and exercises technical control over the brigade signal company in executing the plan. After initializing the local area networks, the S-6 establishes a 24-hour service desk to help with user issues and local area network connectivity in the command posts. Roles and responsibilities of the S-6 include—

- Developing the scheme of signal support to operation orders through the military decision-making process, including PACE plans for each phase of the operation.
- Assist the commander and S-3 in identifying user requirements by number and service type.
- DODIN operations planning for the brigade and subordinate battalions.

- Identifying user requirements by number and service type.
- Spectrum management for the brigade and subordinate battalions.
- Satellite communications planning for the brigade and subordinate battalions.
- Line of sight network planning.
- Tactical radio network planning.
- Tactical radio networks management.
- COMSEC account management.
- Integrating mission command information systems in the brigade network.
- Coordinating, planning, and directing integration of unified action partner networks (mission partner environment).
- Local area network management for the brigade command posts.
- Installing, operating, and maintaining automated information systems and telephone equipment in the brigade command posts.
- Installing, operating, and maintaining Battle Command Common Server.
- Service desk management.
- Helping collect and disseminate relevant input to the common operational picture.
- Supporting the CEMA section, as required.
- Information dissemination management to ensure awareness of relevant, accurate information, automated access to newly discovered or recurring information, and timely information delivery to support decision making.
- Signal maintenance and logistical readiness oversight for communications-electronics equipment.

Brigade Combat Team Signal Company

2-27. The brigade signal company is assigned to the brigade engineer battalion. The company operates under the technical control of the brigade S-6. The company installs, operates, maintains, and secures the brigade's organic network transport, automated information systems, and networks to support command post operations at-the-halt and command and control on-the-move. The signal company employs its platoons and teams throughout the brigade area of operations. The signal company has signal and COMSEC systems maintenance augmentation, spares management, and maintenance accountability from the organic communications-electronics maintenance element of the brigade support battalion's field maintenance company. *Field maintenance* is on-system maintenance, repair and return to the user including maintenance actions performed by operators (FM 4-30).

2-28. The brigade signal company extends information services to the brigade command posts and command vehicles. The brigade signal company also provides—

- Wideband and protected satellite communications transport to connect with the division portion of the DODIN-A.
- High-throughput line of sight transport to communicate between fixed command posts.
- Line of sight and wideband satellite communications transport to support command and control on-the-move.
- Wire, cable, and fiber optic systems to support the brigade and battalion command posts.
- DISN services—SIPRNET, NIPRNET, Joint Worldwide Intelligence Communications System, voice, and video.
- Single-channel radio and narrowband (single-channel) tactical satellite retransmission for the brigade and support elements.
- Global Broadcast Service capability to receive high bandwidth imagery, logistics data, and digital map information to support command and control.

Maneuver Battalion S-6

2-29. The S-6 advises the commander on all matters related to communications in the battalion. The battalion S-6 integrates automated information systems, manages their local area network, implements cybersecurity,

and coordinates spectrum management. Signal planners in the S-6 section are active participants throughout the military decision-making process. The S-6 evaluates the supportability and feasibility of the signal plan supporting each proposed course of action during the military decision-making process. The S-6 maintains the running estimate of communications capabilities and provides signal support plans to design and configure the battalion's communications assets, including PACE plans for each phase of the operation.

2-30. The S-6 interacts closely with the executive officer, S-3, and other staff sections to define communications and network requirements through the military decision-making process. They consult with higher, lower, and adjacent headquarters to ensure effective communications throughout their area of operations. The S-6 should maintain a close working relationship with the commander and battalion S-3 to ensure the communications plan supports the commander's intent. Roles and responsibilities of the S-6 include—

- Developing the scheme of signal support to operation orders through the military decision-making process.
- Assist the commander and S-3 in identifying user requirements by number and service type.
- Identifying user requirements by number and service type.
- Coordinating spectrum management for the battalion's communications systems with the brigade spectrum manager.
- Managing the COMSEC local hand receipt.
- Integrating mission command information systems in the battalion network.
- Local area network management for the battalion command post.
- Installing, integrating, and maintaining automated information systems and telephone equipment in the battalion command post.
- Implements cybersecurity measures to maintain compliant systems.
- Managing tactical radio networks.

Maneuver Battalion Signal Capabilities

2-31. The battalion S-6 section configures, secures, and operates the battalion's organic communications capabilities. Each maneuver battalion has organic tactical radios, local area network, and wide-area network capabilities. The battalion's organic assets support the battalion command post at-the-halt and provide the commander the common operational picture and a command and control on-the-move capability. The battalion S-6 section also provides—

- Beyond line of sight satellite communications access to the division portion of the DODIN-A.
- Line of sight and satellite communications on-the-move to the company, battalion, brigade, and division network.
- DISN services—SIPRNET, NIPRNET, voice, and video.
- Single-channel radio and narrowband (single-channel) tactical satellite communications retransmission for the battalion and support elements.
- Global Broadcast Service capability to receive high bandwidth imagery, logistics data, and digital map information to support command and control.

Maneuver Company Signal Capabilities

2-32. Maneuver companies have limited organic signal capabilities. Companies have single-channel secure radios down to squad level. The company commander has beyond line of sight satellite communications access to the division information network to support the common operational picture, limited DISN services, and command and control on-the-move. The company's communications systems are mostly general-purpose, user-operated equipment not staffed by signal Soldiers. Refer to FM 3-96 for more information about brigade combat team operations.

MULTIFUNCTIONAL SUPPORT BRIGADE

2-33. Combat aviation, field artillery, maneuver enhancement, and sustainment brigades have organic tactical signal assets. Their signal capabilities support the brigade and subordinate battalion command posts operating at-the-halt.

Brigade S-6

2-34. The S-6 advises the commander on all matters related to communications in the brigade. The S-6 advises the commander, staff, and subordinate commanders on technical and training issues related to network and information service integration. The S-6 plans and coordinates signal support to the brigade's main and tactical command posts through the military decision-making process (see appendix B). The brigade S-6 coordinates with the S-3 to direct the actions and movements of signal company elements to support operations through the orders process.

2-35. The S-6 directs planning and coordination for DODIN operations, network transport and information services, and spectrum management for the brigade headquarters and subordinate units. The S-6 collaborates with higher, subordinate, and adjacent units to ensure adequate network support. The S-6 recommends network changes as needed to support the commander's intent.

2-36. The S-6 integrates the brigade's network and information systems. The S-6 prepares the communications plan and exercises technical control over the brigade signal company in executing the plan. After initializing the local area networks, the S-6 section establishes a 24-hour service desk to help with user issues and local area network connectivity in the command posts. Roles and responsibilities of the S-6 include—

- Developing the scheme of signal support to operation orders through the military decision-making process, including PACE plans for each phase of the operation.
- Assist the commander and S-3 in identifying user requirements by number and service type.
- DODIN operations planning for the brigade and subordinate battalions.
- Satellite communications planning for the brigade and subordinate battalions.
- Line of sight network planning.
- Tactical radio network planning.
- Spectrum management for the brigade and subordinate battalions.
- COMSEC account management.
- Integrating mission command information systems in the brigade network.
- Coordinating, planning, and directing integration of unified action partner networks (mission partner environment).
- Local area network management for the brigade command posts.
- Service desk management.
- Helping collect and disseminate relevant input to the common operational picture.
- Supporting the CEMA section, as required.
- Information dissemination management to ensure awareness of relevant, accurate information, automated access to newly discovered or recurring information, and timely information delivery to support decision making.
- Signal maintenance and logistical readiness oversight for communications-electronics equipment.

Brigade Signal Company

2-37. The brigade signal company operates under the technical control of the brigade S-6. The company installs, operates, maintains, and secures the brigade's network transport, automated information systems, and networks. The brigade's organic signal capabilities support command post operations at-the-halt. The brigade signal company has signal maintenance augmentation, spares management, and maintenance accountability from the brigade's organic communications-electronics maintenance element. Either the organic maintenance element or the support maintenance company provides remaining maintenance support

for communications-electronics, COMSEC, automotive, power generation, and environmental control equipment.

2-38. The brigade signal company supports the brigade and subordinate battalion command posts. The brigade signal company also provides—

- Wideband and protected satellite communications transport to connect with the division portion of the DODIN-A.
- High-throughput line of sight transport to communicate between command posts.
- Line of sight and wideband satellite communications transport to support command and control on-the-move.
- DISN services—SIPRNET, NIPRNET, Joint Worldwide Intelligence Communications System, voice, and video.
- Single-channel radio and narrowband (single-channel) tactical satellite retransmission for the brigade and support elements.
- Global Broadcast Service capability to receive high bandwidth imagery, logistics data, and digital map information to support command and control.
- Wire, cable, and fiber optic systems to support the brigade and battalion command posts.

Battalion S-6

2-39. The battalion S-6 integrates automated information systems, manages the battalion local area network, implements cybersecurity, and coordinates spectrum management. Signal planners in the S-6 section are active in the operations process. The S-6 ensures the commander can communicate to exercise command and control. The S-6 evaluates the supportability and feasibility of the signal plan supporting each proposed course of action during the military decision-making process. The S-6 maintains the running estimate of communications capabilities and provides signal support plans to build and configure the battalion's communications capabilities.

2-40. The S-6 interacts closely with the executive officer, S-3, and other staff sections to define communications and network requirements through the military decision-making process. They collaborate with higher, lower, and adjacent headquarters to ensure effective communications throughout their area of operations. The S-6 should maintain a close working relationship with the commander and battalion S-3 to ensure the communications plan supports the commander's intent. Roles and responsibilities of the S-6 include—

- Developing the scheme of signal support to operation orders through the military decision-making process, including PACE plans for each phase of the operation.
- Assist the commander and S-3 in identifying user requirements by number and service type.
- Coordinating spectrum management for the battalion's communications systems with the brigade spectrum manager.
- Managing the battalion COMSEC hand receipt.
- Managing tactical radio networks.
- Integrating mission command information systems in the battalion network.
- Local area network management for the battalion command post.
- Installing, integrating, and maintaining automated information systems and telephone equipment in the battalion command post.
- Implementing cybersecurity measures to maintain compliant systems.

2-41. The S-6 section performs local area network setup, administration, and user support. Attached brigade signal company elements provide only the connection to DISN services. Refer to ATP 6-02.60 for more information about brigade through corps communications.

SECURITY FORCE ASSISTANCE BRIGADE

2-42. Each security force assistance brigade, both armored and infantry variants, has two maneuver battalions, a cavalry squadron, a field artillery battalion, an engineer battalion, a military intelligence company, a signal company, a support battalion, and a headquarters and headquarters company (ATP 3-96.1).

Brigade S-6

2-43. The S-6 advises the commander on all matters related to communications in the brigade. The S-6 advises the commander, staff, and subordinate commanders on technical and training issues related to network and information service integration. The S-6 plans and coordinates signal support to the brigade's main and tactical command posts through the military decision-making process (see appendix B). The S-6 collaborates with subordinate battalion S-6s and supported unit to ensure adequate network support. See appendix B for more information about collaboration with higher and subordinate signal elements.

Brigade Signal Company

2-44. The signal company provides voice and data retransmission capability for its tactical radio network. The retransmission team provides line of sight extension of the brigade's tactical radio network within the brigade area of operations. During deployment, the signal company uses augmented assets from the expeditionary signal battalion to provide worldwide digital voice and data communications to enable command and control across the brigade's area of operations.

Battalion S-6

2-45. The battalion S-6 coordinates with the brigade S-6 to define communications and network support requirements, based on the situation and mission. The operational chain of command validates requests for signal support they cannot source internally and forwards them to United States Army Forces Command for approval and resourcing. The supporting signal unit provides a communications package tailored to validated communications and information exchange requirements.

UNITS WITHOUT ORGANIC SIGNAL ASSETS

2-46. Theater tactical signal brigades and their assigned expeditionary signal battalions, are manned, trained, and equipped to provide communications support to expeditionary units with no organic signal assets. See paragraph 2-57 for more information about the theater tactical signal brigade.

THEATER ARMY

2-47. The theater army is the Army Service component command to a geographic combatant command. The theater army headquarters—

- Exercises administrative control of all Army forces in the geographic combatant command area of responsibility.
- Integrates Army forces into theater engagement plans.
- Provides Army support to joint, interorganizational, and multinational forces, as directed by the geographic combatant commander.

2-48. The theater army main command post conducts routine day-to-day operations and crisis action planning. With augmentation, the contingency command post can deploy to conduct small-scale operations, commanding up to two brigade combat teams or equivalent for up to 30 days.

2-49. The theater army is designated as the DOD executive agent for setting and supporting the theater communications and network architecture. The theater army executes these executive agent responsibilities primarily through a signal command (theater) [SC(T)] assigned to support the area of responsibility (ATP 3-93). Each Service component in a joint task force maintains its own networked communications infrastructure, compatible with the other unified action partners. The J-6 exercises staff oversight over the Service component systems in the joint force. The Service components may need to provide staffing or equipment augmentation for the joint task force J-6 section.

Theater Army G-6

2-50. The theater army G-6 plans, prioritizes, and coordinates communications and automated information systems requirements to support Army units in a theater of operations. The G-6 integrates information systems support to geographic combatant commander-designated joint, interorganizational, and multinational partners. The G-6 assesses the network's ability to meet the commander's requirements and develops relevant parts of operation orders, operation plans, and concept plans. The theater army G-6 validates communications and information systems requirements and urgent operational needs statements for Army units in theater, and makes recommendations for resourcing.

- **Headquarters section.** Supervises planning, requirements development, and information management policy for information systems support for the theater army headquarters and Army forces in theater.
- **Operations section.** G-6 operations coordinates with military and civil communications authorities of the host nation and integrates information systems support to geographic combatant commander-designated joint, interorganizational, and multinational partners. The operations section validates information system requirements and service requests to support Army forces in theater. The section develops information system requirements to support Army and joint exercises, and plans, implements, and analyzes information system requirements for the headquarters.
  - **COMSEC account manager.** The COMSEC account manager maintains the theater army headquarters COMSEC account, establishes COMSEC operations policies, and enforces policies in the theater army area of operations. The COMSEC account manager also provides user-level training on COMSEC material management and accountability.
  - **Spectrum element.** The spectrum element coordinates with other spectrum managers to integrate Army and joint systems with the headquarters network. The element coordinates, manages, and apportions frequency assignments for land forces in theater. The spectrum manager coordinates with host-nation spectrum authorities to deconflict military use of the electromagnetic spectrum.
- **Programs, policy, and projects headquarters section.** The programs, policy, and projects headquarters section of the main command post plans and controls the headquarters' information management architecture and long-range modernization plans. The section tracks the status of the headquarters' automated information systems and local area network. The section develops and justifies long-range financial plans, and conducts research and analysis to evaluate technology available to support user requirements.
  - **Projects branch.** The projects branch manages network initiatives and projects for the theater army headquarters. The branch manages intra-theater information system projects, programs, and initiatives and integrates commercial off-the-shelf communications and information systems into the theater network. The branch coordinates with national- and strategic-level information systems engineering activities to implement information technology initiatives in support of theater army operations and plans.
  - **Cybersecurity branch.** The cybersecurity branch establishes, manages, and assesses the headquarters' cybersecurity program. The branch provides user-level cybersecurity awareness training to help secure the network infrastructure and oversees, assesses, and supports information technology systems accreditation according to the DOD risk management framework. Refer to DODI 8510.01 for detailed information about the DOD risk management framework.
  - **Programs and policy branch.** The programs and policy branch plans and controls theater army headquarters basing initiatives, information management architecture, and long-range modernization plans. The branch develops and justifies long-range financial plans that support users' information system requirements.
  - **Enterprise architecture branch.** The enterprise architecture branch ensures compliance and interoperability of the Army information technology architecture within the theater, in support of the regional cyber center. The branch manages the theater portion of the Army information management program to support network-enabled, knowledge-based operations. The

enterprise architecture branch also develops theater enterprise architecture and standards to ensure equipment, systems, and networks meet DOD, joint, Department of the Army and other applicable operational and doctrinal requirements.

- **Headquarters support section.** The headquarters support section installs, operates, maintains, and secures video teleconferencing services and local area networks to support headquarters users, and protects headquarters information systems from cyberspace attack. The section defines requirements for communications, automated information systems, and services and manages the headquarters information systems automation life cycle replacement plan.
- **Joint and coalition network section.** The joint and coalition network section plans, and coordinates the management of, joint functional computer systems—both hardware and software. The section integrates joint information systems with command post and sustainment information systems. The section develops the information management plan and maintains Global Command and Control System (Army and joint) servers to provide the common operational picture for the theater army area of operations. The section represents the theater army on Army, joint, and multinational information management boards. The section also develops and maintains the concept of operations for multinational network information exchange, develops network architecture and support requirements for joint and multinational exercises, and plans implementation for new technologies.

Signal Support

2-51. The theater army has no organic signal capabilities. The theater army headquarters receives its network and information services support from the local network enterprise center. If the theater army deploys a contingency command post, the command post receives signal support from theater-committed or rotational signal units. The theater Army G-6 identifies requirements, and the G-3 requests support through the geographic combatant commander to United States Army Forces Command. The pooled resources of a theater tactical signal brigade normally fulfill these communications requirements. See appendix E for more information about requests for signal support.

FUNCTIONAL SUPPORT BRIGADES

2-52. A functional support brigade is a brigade or group that provides a single function or capability. These brigades can provide support for a theater, corps, or division, depending upon how each is tailored (FM 3-94). Functional support brigades receive their signal support either from the organic assets of the supported unit or from pooled assets, such as an expeditionary signal battalion or forward operating base infrastructure, as defined in the operation order. The supported unit assumes DODIN operations responsibility for the support brigade. Managing the network may require augmentation.

2-53. The support brigade S-6 coordinates with the supported unit's G-6 (S-6) to define communications and network support requirements, based on the situation and mission. The operational chain of command validates requests for signal support they cannot source internally and forwards them to United States Army Forces Command for approval and resourcing. The signal support unit provides a communications package tailored to satisfy validated communications and information exchange requirements.

JOINT TASK FORCES

2-54. Combatant commanders tailor task forces based on the commander's vision, the concept of operations, the situation, and the mission. As an ad hoc headquarters, a joint task force has no organic capabilities. The commander, joint task force can task any force component to provide communications and network support for the headquarters. The commander, joint task force controls joint task force communications systems and networks through a joint network operations control center. Refer to JP 6-0 for more information about the joint network operations control center.

2-55. The Army component of the joint task force provides its own communications support using organic or pooled signal capabilities. The Army component of the joint task force is directly subordinate to the commander, joint task force or joint force land component commander, but under the administrative control of the theater army. The Army component headquarters has a dual DODIN operations reporting

relationship—to the joint task force (through the joint network operations control center) and the theater army (through the regional cyber center).

2-56. The commander, joint task force exercises overall authority and responsibility for DODIN operations within the joint operations area. The theater army also provides guidance to Army forces through technical channels to ensure compliance with Army policies for DODIN operations. Refer to JP 3-33 for more information about joint task force operations.

SIGNAL COMMAND (THEATER)

2-57. The SC(T) headquarters at its home station receives communications and information services support from its local network enterprise center. Forward deployed SC(T) staff elements receive network and information services support through an overseas installation's network enterprise center or forward operating base infrastructure, or request communications support from theater-committed or rotational signal units through the geographic combatant commander to United States Army Forces Command.

Note. In a theater with no assigned SC(T), the strategic signal brigade commander and staff or the tactical actions center assume the staff functions normally associated with the SC(T).

TYPES OF SIGNAL UNITS LEVERAGED FOR SUPPORT

2-58. The Army's global force pool includes echelons above core expeditionary signal units to support those units with no organic signal assets. Expeditionary signal units can also augment corps and below units when organic capabilities are not sufficient for an assigned mission.

THEATER TACTICAL SIGNAL BRIGADE

2-59. The theater tactical signal brigade headquarters supervises building, configuration, operation, and maintenance of communications nodes, and secures these nodes, in the deployed portion of the network, excluding the division and corps systems. It also integrates interorganizational and multinational partners into the DODIN. The theater tactical signal brigade—

- Allocates, controls, and positions tactical networking resources.
- Oversees connection to the network for Army and designated joint, interorganizational, and multinational elements.
- Provides physical security for, and actively defends, network resources.
- Performs long-range planning for tactical network expansion and upgrade.
- Enforces global (enterprise) and theater-level technical standards and policies for assigned tactical networking resources.
- Conducts enterprise systems management and network management.
- Conducts spectrum management operations for tactical signal forces in theater.
- Exercises communications-electronics maintenance and logistical readiness oversight over subordinate elements.
- Oversees contractor support operations and personnel.

Expeditionary Signal Battalion

2-60. The expeditionary signal battalion is a fundamental building block of the Army's global force pool. Most expeditionary signal battalions are theater available forces that can deploy for contingency or enduring missions. An expeditionary signal battalion consists of a headquarters company, two expeditionary signal companies, and a joint/area signal company. The battalion headquarters provides administrative and logistical support for the signal battalion. The battalion S-3 oversees designing, building, configuring, securing, operating, maintaining, and sustaining nodal and extension communications.

2-61. The expeditionary signal battalion supports Army units up to theater army, joint force land component commanders, or joint task force headquarters. It also manages tactical communications assets in the battalion through its suite of DODIN operations tools. The battalion headquarters provides these capabilities—

- Staff planning and supervision of the battalion and any attached units.
- Field maintenance support for the battalion headquarters.
- COMSEC account management for the battalion.
- Field maintenance of organic COMSEC equipment.

Note. COMSEC repair authorities cannot be delegated. Typically, field maintenance of COMSEC is limited to preventive maintenance checks and services, inspection, detection, and correction of minor faults.

Expeditionary Signal Company

2-62. The expeditionary signal company headquarters provides staff planning and supervision of its signal platoons and any augmenting elements, personnel, or material assets. The expeditionary signal company provides communications support in theater primarily for echelons above corps Army units. The expeditionary signal company may also support other units without organic signal capabilities or augment a unit's organic capabilities. The expeditionary signal company also provides—

- Wideband and protected satellite communications transport.
- Beyond line of sight troposcatter network transport.
- High-throughput line of sight transmission.
- Telephone switching services.
- DODIN operations tools to support network management within the company.
- Cable, wire, and fiber optic installation and maintenance.
- Access to DISN voice, data, and video services.
- Field maintenance support for organic communications-electronics, COMSEC, automotive, power generation, and environmental control equipment.

Joint/Area Signal Company

2-63. The joint/area signal company installs, operates, maintains, and secures large or medium command nodes to extend DISN services supporting Army and joint missions in a theater of operations. The company can also provide limited DISN services to support smaller command posts. This support includes line of sight and beyond line of sight network transport, network management, and cable and wire installation to provide garrison-quality data services to deployed users. The joint/area signal company primarily supports large headquarters command posts, such as a geographic combatant command, theater army, joint task force, or joint force land component command. The company can also support a limited number of battalion-sized command posts. This joint/area signal company provides—

- Large command post support—DISN services.
- High-throughput line of sight transmission.
- Small command post support—limited DISN services.
- DODIN operations tools to support network management within the company.
- Troposcatter network transport to link large command posts, major headquarters, and signal nodes.
- Wideband satellite communications transport.
- Protected satellite communications connectivity between selected large and small node centers and remote command posts.
- Cable and multiplexer assets to interconnect signal equipment.
- Field maintenance and limited sustainment maintenance of organic communications-electronics and COMSEC equipment.

SPECIAL-PURPOSE SIGNAL UNITS

2-64. The Army's global force pool contains single-purpose signal units designed to concentrate low-density specialties. Units can request the specialized support these signal companies provide through their operational chain of command to United States Army Forces Command.

Combat Camera Company

2-65. The combat camera (COMCAM) company provides visual documentation covering the Military Services in war, natural disasters, and training activities. The company provides still and motion imagery and video documentation to support intelligence and decision making. The COMCAM company provides—

- Liaison to supported units, joint COMCAM teams, and other Service COMCAM elements.
- Planning, coordination, and supervision of COMCAM documentation support missions.
- COMCAM support for airborne operations (airborne COMCAM company only).
- COMCAM support for ground, air assault, and amphibious operations.
- Still photo (film and digital) and video editing, including rough editing for on-site customers.
- Tailored still and motion media, graphics products, narration support, video reports, presentations, and visual imagery to support operational headquarters in the theater army, corps, and division areas of operation.
- COMCAM equipment maintenance by on-site repair, replacement, or evacuation to civilian contractors.
- Field maintenance of vehicles, power generators, environmental control units, and signal support systems.

Tactical Installation and Networking Company-Enhanced

2-66. The tactical installation and networking company-enhanced provides network installation, troubleshooting, quality assurance testing, and handoff coordination to enable the transition from tactical to semi-permanent automation support. The company provides these capabilities to support theater army, geographic combatant command, SC(T), and joint task force or coalition headquarters:

- Installation, maintenance, troubleshooting, testing, and repair of cable, wire, and fiber optic transmission systems.
- Antenna and tower construction and repair.
- Installation of automated information systems and services, including—
  - Local area networks.
  - Wide-area networks.
  - Network security hardware.
  - SIPRNET.
  - NIPRNET.
  - Video teleconferencing.

2-67. The tactical installation and networking company-enhanced headquarters performs these functions to support the unit's mission:

- Advice to supported commanders on all aspects of network installation, including inside and outside plant, local area networks, and wide-area networks.
- Technical expertise to interpret and execute engineering implementation plans for communications systems.
- Direction and technical expertise to cable and wire sections and teams to restore supported facilities.
- Planning, coordination, configuration, and integration of network installation efforts.

REQUESTING SIGNAL SUPPORT

2-68. A requesting unit's G-6 (S-6) defines signal support requirements based on the mission, size of the operation, the number of personnel and systems, and services needed. Signal requirements are not static; they may change with the operational and mission variables. When defining requirements, the requesting unit describes—

- The unit needing service and the number of connections needed for each requested service.
- The services needed—NIPRNET, SIPRNET, voice, special circuits, and COMSEC key support.
- The date-time group for required services.
- The location for required services.
- The supported unit battle rhythm for communications services.

2-69. Requests for signal support route through the operational chain of command to United States Army Forces Command for validation and resourcing. When supporting a division, the requesting unit's S-6 and S-3 coordinate through the division G-6 to the theater army G-6 to identify and validate support requirements. Any unit not tasked to a division coordinates directly with the theater army G-6 to request signal support.

2-70. When the operation order identifies the supporting signal unit, the requesting G-6 (S-6) contacts that unit for coordination. The supporting signal unit provides the connection to DISN services, but does not provide computers, telephones, or local area network support.

2-71. Supporting signal assets may fall under the operational or tactical control of the supported unit. The supported unit may assume responsibility to provide logistics, personnel services, and health service support, based on the command relationship established in the deployment order. See appendix E for details about requests for signal support.

SUPPORT TO OTHER ARMY OPERATIONS

2-72. Certain types of Army units have organic signal capabilities to support their unique missions. Some types of Army operations have specific communications requirements. Expeditionary signal units support these operations.

SUPPORT TO ELECTRONIC WARFARE

2-73. *Electronic warfare* is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (JP 3-13.1). The DODIN-A supports planning and coordination of EW activities. The unit's DODIN operations personnel, spectrum manager, and G-6 (S-6) staff perform key roles in EW planning.

2-74. The unit's network and automated information systems support EW planning. Signal Soldiers provide the network for EW planners to—

- Prepare electronic protection policy on behalf of the commander.
- Prepare EW plans and orders.
- Aggregate EW sensor data to detect enemy electronic attacks.
- Report enemy electronic attack activity on friendly networks.
- Help resolve issues with EW systems maintenance or interference with friendly communications.

2-75. The spectrum manager in the G-6 (S-6) coordinates electromagnetic spectrum use for communications and other electronic resources. Some units have spectrum managers in both the signal staff and the EW section. The spectrum managers support EW by—

- Coordinating spectrum resources for the unit or task force.
- Coordinating spectrum use with higher echelon G-6 (S-6), host-nation spectrum authorities, and international agencies, as necessary.
- Preparing the restricted frequency list.
- Issuing emissions control guidance.

- Coordinating with the cyber electronic warfare officer for electromagnetic deception plans in which assigned communications elements participate.
- Coordinating measures to reduce electromagnetic interference.
- Coordinating with higher echelon spectrum managers to mitigate electromagnetic interference that cannot be resolved internally.
- Helping the cyber electronic warfare officer issue guidance to deconflict and resolve interference between EW systems and friendly communications.
- Participating in CEMA to deconflict friendly electromagnetic spectrum requirements with planned EW operations and information collection.

SUPPORT TO INTELLIGENCE OPERATIONS

2-76. The deployed portion of the DODIN-A provides network transport for intelligence-unique automated information systems. These systems gather intelligence spanning all echelons and warfighting domains and enable operational visualization and situational awareness for current and future operations. These intelligence systems give commanders the ability to view joint intelligence, surveillance, and reconnaissance products in one place and integrates that information into tools that can support intelligence development.

2-77. With transport convergence (see paragraph 2-267), the deployed network also provides network transport for the top secret/sensitive compartmented information network to the brigade level. While the network transport takes place through the tactical signal systems, the G-2 (S-2) section continues performing DODIN operations for the top secret network.

SUPPORT TO SPACE OPERATIONS

2-78. The Army relies on space-based capabilities and systems, such as global positioning, communication, weather satellites, and intelligence collection platforms. These systems are critical enablers used by the corps to plan, communicate, navigate, maneuver, maintain situational awareness, engage the enemy, provide missile warning, protect, and sustain forces (FM 3-14). One of the Army's key space capabilities is satellite communications. Specially-trained signal Soldiers plan, manage, monitor, and control access to the Defense Satellite Communications System and Wideband Global Satellite Communications constellations (see paragraph 2-161). Refer to FM 3-14 for more information about Army space operations. Refer to ATP 6-02.54 for more information about satellite communications.

SUPPORT TO SPECIAL OPERATIONS

2-79. Army special operations forces require a secure and robust communications system to ensure the commander can exercise authority and direct forces over large geographic areas. Special forces and Rangers' organic signal capabilities provide communications and network services tailored to their unique requirements.

2-80. Special operations communications networks include redundant transmission paths to prevent site isolation. Global communications support ensures Army special operations forces can communicate anywhere and at any time using strategic capabilities to the maximum extent possible, as well as commercial, tactical, and host-nation assets (ATP 3-05.60).

Special Forces

2-81. The Army special operations forces location, mission, and structure drive specific information requirements and flow, processing requirements and the specific configuration of the communications system. Connectivity throughout the operational area is vital to planning, conducting, and sustaining operations. The communications system must be tactically agile and globally deployable with consideration made for communications that are en route, within the area of responsibility, and between the areas of responsibility (ATP 3-05.60).

2-82. The special operations communications system meets these unique requirements with a blend of standard Army communications capabilities, commercial off-the-shelf systems, and special operations forces-specific capabilities.

Special Forces Group

2-83. Each special forces group has an S-6 with a supporting section located in the group headquarters and headquarters company, and a group signal detachment located within the group special troops battalion. Each special forces battalion has an S-6, with a supporting section located in the battalion headquarters and a battalion signal detachment located in the battalion support company (ATP 3-05.60).

2-84. The group S-6 prepares signal plans; conducts information management, spectrum management operations, and COMSEC management; and supports EW operations focusing on electronic protection. The special forces group's organic signal capabilities include—

- Wideband satellite communications.
- Special operations forces-unique switching systems.
- Tactical local area network—connected to either the DISN or the closed special operations forces network.
- Mission command information systems.
- Global Broadcast Service.
- Narrowband (single-channel) satellite communications.
- Single-channel radios.
- Line of sight radios.
- Satellite telephones.
- International maritime satellite Broadband Global Area Network.

2-85. The battalion S-6 advises the commander on signal support, automation management, DODIN operations, and information security. The duties of the battalion S-6 are similar to the group S-6. Special forces battalion capabilities include—

- Wideband satellite communications.
- Special operations forces-unique switching systems.
- Tactical local area network—connected to either the DISN or the closed special operations forces network.
- Mission command information systems.
- Narrowband (single-channel) satellite communications.
- Single-channel radios.
- International maritime satellite Broadband Global Area Network.

2-86. Special forces operational detachments A and B have organic narrowband satellite communications, single-channel radio, international maritime satellite Broadband Global Area Network, satellite telephone, and friendly force tracking capabilities.

Special Operations Signal Battalion

2-87. The special operations signal battalion provides operational- and tactical-level communications to support joint and Army special operations forces. The battalion network operations and security center manages the Army special operations forces tactical network.

2-88. The special operations signal battalion provides these capabilities:

- DODIN operations for the Army special operations forces network.
- Planning, installing, operating, and maintaining the theater-level special operations forces wide-area network.
- Classified and unclassified voice, video, and data communications to support early or forcible entry and sustained command post operations for United States Army Special Operations Command. The battalion can also perform this function to support a joint task force or joint special operations task force.
- Reachback to special operations forces headquarters to support split-based operations.
- Configuration management to maintain interoperability with the rest of the DODIN.
- COMSEC account management and maintenance.

- Field- and sustainment-level maintenance for organic signal equipment and automation systems.
- Limited maintenance of special operations forces-unique signal equipment.
- Communications support for airborne and airdrop operations.

Rangers

2-89. The Ranger Regiment's organic signal company deploys worldwide to install, operate, maintain, and secure the regiment's communications and automated information systems. The Ranger Regiment signal company establishes secure networks to support the regiment's operations and integrate with the Army force component of a joint force. The signal company provides local area network support for the company, the Ranger battalions, the Ranger Special Troops Battalion, and the Ranger Regiment.

2-90. The Ranger Regiment signal company provides—

- Automated information systems support for maneuver, support, and command elements.
- Tactical radio relay, retransmission, and beyond line of sight high frequency and single-channel satellite communications to extend networks.
- Global Broadcast Service capability to receive high bandwidth imagery, logistics data, and digital map information to support command and control.
- Field- and sustainment-level communications-electronics and COMSEC maintenance for the special troops battalion and supporting organizations.

SUPPORT TO CYBERSPACE OPERATIONS

2-91. *Cyberspace operations* are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace (JP 3-0). The core cyberspace operations missions are—

- DODIN operations.
- Defensive cyberspace operations.
- Offensive cyberspace operations.

2-92. Cyberspace actions support DODIN operations, defensive cyberspace operations, offensive cyberspace operations, or any combination thereof. Executing cyberspace actions at any echelon is dependent on authority, capability, and coordination. The cyberspace actions are interrelated. A cyberspace mission may require more than one action to achieve mission success. The cyberspace actions are—

- Cyberspace defense.
- Cyberspace intelligence, surveillance, and reconnaissance.
- Cyberspace operational preparation of the environment.
- Cyberspace attack.
- Cyberspace security.

2-93. Signal support to cyberspace operations includes the tasks to establish the baseline security posture and operate the DODIN-A. Signal Soldiers perform DODIN operations to support both the joint and Army portions of cyberspace and take part in CEMA.

2-94. Cyberspace security actions are those taken within a protected network. Cyberspace security actions prevent unauthorized access to, an exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology. Cyberspace security actions help ensure the availability, integrity, authentication, confidentiality, and nonrepudiation of classified and other sensitive information. Cyberspace security is not specific to an enemy or adversary. Cyberspace security actions protect the networks and systems through all phases of network planning and implementation. Cyberspace security activities include vulnerability assessment and analysis, vulnerability management, incident handling, continuous monitoring, and detection and restoration capabilities to shield and preserve information and information systems (FM 3-12). Refer to FM 3-12 for more information about the other cyberspace actions.

Department of Defense Information Network Operations

2-95. The cyberspace operations mission of DODIN operations is primarily a signal support function. *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). DODIN operations functions include routine activities to operate the network and establish the baseline cybersecurity framework.

Support to Defensive Cyberspace Operations

2-96. *Defensive cyberspace operations* are missions to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity (JP 3-12). Most defensive cyberspace operations tasks at corps and below focus on enabling friendly command and control and fires while protecting the DODIN. Adversaries and enemies continuously seek to gain an advantage by penetrating friendly networks to disrupt operations. Army units conduct defensive cyberspace operations to prevent, detect, identify, and respond to anomalous or unauthorized activity, intrusions, or attacks against the DODIN and other networks when authorized.

Defensive Cyberspace Operations-Internal Defensive Measures

2-97. *Defensive cyberspace operations-internal defensive measures* are operations in which authorized defense actions occur within the defended portion of cyberspace (JP 3-12). Most defensive cyberspace operations missions are defensive cyberspace operations-internal defensive measures, which include pro-active and aggressive internal threat hunting for advanced and/or persistent threats, as well as the active internal countermeasures and responses used to eliminate these threats and mitigate their effects (JP 3-12). Defensive cyberspace operations-internal defensive measures are responses to unauthorized activity, alerts, or threat information within the defended network. Defensive cyberspace operations-internal defensive measures leverage intelligence, counterintelligence, law enforcement, and other military capabilities, as required.

2-98. For compromised DODIN elements, specific tactics include rerouting, reconstitution, restoration, or isolation. To defend cyberspace, signal personnel work to detect, analyze, and respond to unauthorized activities not mitigated by cybersecurity measures. United States Army Cyber Command (ARCYBER) is the Army lead for defensive cyberspace operations-internal defensive measures. Cyberspace defenders and DODIN operations personnel apply mitigation measures recommended by cyber protection teams.

Defensive Cyberspace Operations-Response Actions

2-99. *Defensive cyberspace operations-response actions* are operations that are part of a defensive cyberspace operations mission that are taken external to the defended network or portion of cyberspace without the permission of the owner of the affected system (JP 3-12). Because the actions occur outside the DOD network, defensive cyberspace operations-response actions are subject to legal constraints and restraints. Defensive cyberspace operations-response actions require authorization according to standing and supplemental rules of engagement. To support response actions, signal personnel help identify key terrain in cyberspace during CEMA. Security logs collected as part of DODIN operations help identify threat actions and feed planning for defensive cyberspace operations-response actions. Signal Soldiers and units provide the network (the DODIN-A) used for defensive cyberspace operations-response actions planning and targeting requests.

Support to Offensive Cyberspace Operations

2-100. *Offensive cyberspace operations* are cyberspace operations intended to project power by the application of force in or through cyberspace (JP 3-12). Army units plan, synchronize and integrate offensive cyberspace operations to create effects supporting commanders' objectives. Signal Soldiers and units provide the network (the DODIN-A) used for offensive cyberspace operations targeting requests.

Synchronizing Department of Defense Information Network Operations and Defensive Cyberspace Operations

2-101. Defensive cyberspace operations and DODIN operations share a common objective of a secure network. DODIN operations tasks are network-focused. Cybersecurity sets the baseline security posture of the network to protect against known exploits and vulnerabilities, rather than a particular threat actor or capability. The cybersecurity workforce attempts to mitigate all vulnerabilities of their assigned network or systems. Cybersecurity uses available intelligence about specific threats to improve the network's security posture.

2-102. By contrast, defensive cyberspace operations are mission-focused and threat-specific. Defensive cyberspace operations missions involve deliberate measures to counter a specific threat attack, exploitation, or malware that has breached security measures. Defensive cyberspace operations leverage information from intelligence, counterintelligence, law enforcement, and other sources, as required.

Cyberspace Electromagnetic Activities

2-103. Commanders and staffs face the challenge of enabling joint, interorganizational, and multinational collaboration and assuring access to critical data and information networks in increasingly congested and contested cyberspace and electromagnetic spectrum environments, while simultaneously denying the same to the enemy. Operating in the congested and contested information environment requires commanders and their staffs to synchronize signal, cyberspace, and EW capabilities through CEMA. *Cyberspace electromagnetic activities* is the process of planning, integrating, and synchronizing cyberspace and electronic warfare operations in support of unified land operations (ADP 3-0).

2-104. CEMA integrates—

- Cyberspace operations.
  - DODIN operations.
  - Defensive cyberspace operations.
  - Offensive cyberspace operations.
- EW.
  - Electronic attack.
  - Electronic protection.
  - Electronic warfare support.
- Spectrum management operations.

2-105. Because the hybrid threat integrates information warfare capabilities in these areas, U.S. forces must similarly coordinate their defenses. Attempting to conduct signal, cyberspace, and EW activities in isolation makes them more vulnerable. Synchronizing these activities through CEMA ensures coordinated defense and counter-offense against threat information warfare activities.

2-106. To support CEMA at the theater army level and below, the G-6 (S-6) staff and spectrum manager integrate DODIN operations and spectrum management actions. They also coordinate to synchronize these actions with mutually supporting capabilities residing in the G-2 (S-2) and G-3 (S-3) sections.

2-107. Signal, cyberspace, and EW missions share certain areas of potential overlap. Each has its own set of threat and performance indicators. Synchronizing signal, cyberspace, and EW missions and tasks strengthens all of them beyond their inherent capabilities.

2-108. Shared awareness between signal, cyberspace operations, EW, and intelligence elements improves situational understanding and identifies opportunities for mutual support between the capabilities. The CEMA section coordinates to deconflict spectrum use between signal and EW elements. Deconfliction ensures EW capabilities do not create unintended electromagnetic interference (frequency fratricide) with friendly communications, unmanned aircraft systems, weapon systems, or positioning, navigation, and timing. Failing to share situational understanding could cause planners or operations personnel to miss indicators of a cyberspace or electronic attack. The EW section can plan and execute electronic attack and electronic protection actions to support signal capabilities.

2-109. Synchronizing signal, cyberspace, EW, and intelligence capabilities is especially important when planning for, or operating against, a peer threat. Refer to FM 3-12 for more information about cyberspace operations and CEMA. Refer to ATP 3-12.3 for more information about EW techniques.

Cyberspace Workforce Management

2-110. DOD policy unifies the cyberspace workforce to align, manage, and standardize roles, qualifications, and training requirements for—

- Cyberspace effects elements.
- Cybersecurity elements.
- Cyberspace information technology elements.
- Intelligence workforce (cyberspace).

2-111. Personnel in the cyberspace workforce must meet minimum qualifications based on their respective cyberspace roles. While the policy standardizes the workforce requirements, the Joint Staff, combatant commands, and Services base their operational employment decisions on mission requirements. Refer to DODD 8140.01 for more information about cyberspace workforce management.

ENABLING INFORMATION AND KNOWLEDGE MANAGEMENT

2-112. It is essential that the joint communications system complement human capabilities and reduce or eliminate anticipated or known limitations to mission accomplishment (JP 6-0). Improved technology in mobility, weapons, sensors, and communications generates large amounts of data with which to establish situational understanding. However, the volume of data can overwhelm planners and decision makers, leading to poor decisions. For the data to be useful, staffs need to process and analyze it into relevant information and knowledge so the commander and staff can achieve understanding.

2-113. Information, as an element of combat power, includes both the combat information necessary to gain understanding and make decisions and the use of information to dominate the information environment. Information enables commanders at all levels to make informed decisions on how best to apply combat power. Well-managed information and knowledge lead to a distinct information advantage. Through information and knowledge management, the right information gets to the right people to support better decision making.

Information Management

2-114. *Information management* is the science of using procedures and information systems to collect, process, store, display, disseminate, and protect data, information, and knowledge products (ADP 6-0). Information management helps commanders make and disseminate effective decisions faster than the enemy can. Signal personnel conduct information management. They perform these information management tasks to enable knowledge management:

- Application and database administration.
- Data backup and migration.
- Website interface maintenance.
- Troubleshooting.
- Security.
- Configuration.
- Providing network architecture and technological tools to support content management and content sharing.
- Providing DODIN operations and information management support through the G-6 (S-6) section.

Knowledge Management

2-115. Well-managed information enables knowledge management. *Knowledge management* is the process of enabling knowledge flow to enhance shared understanding, learning, and decision making (ADP 6-0). Knowledge management enables commanders to make informed, timely decisions despite the uncertainty of

operations. Knowledge management aligns an organization's people, processes, and tools to distribute knowledge and promote shared situational understanding.

2-116. Signal Soldiers assigned to the knowledge management section ensure the information technology network supports knowledge creation and uses automated knowledge management tools. Some signal Soldiers serve in the knowledge management section. Their responsibilities include providing software developer capability support. Refer to ATP 6-01.1 for more information about knowledge management.

SUPPORT TO INFORMATION OPERATIONS

2-117. *Information operations* are the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own (JP 3-13). Some information-related capabilities (COMCAM, satellite communications, and DODIN operations) are Signal Corps functions.

2-118. The DODIN-A provides a platform to plan information operations and synchronize information-related capabilities globally across all echelons and organizations in near real-time. Security and defense of the DODIN-A through cybersecurity and defensive cyberspace operations provide a layer of defense against threat information warfare capabilities.

SUPPORT TO AVIATION OPERATIONS

2-119. Combat aviation brigades have organic signal Soldiers and capabilities to support deployed forces (see paragraph 2-31). These organic capabilities connect the brigade and battalion command posts to the DODIN-A.

2-120. The DODIN-A also provides network transport for aviation-specific automated information systems. These systems integrate air and ground operations, facilitate civil and interagency airspace coordination, and provide joint interoperability with the joint force air component commander. Interoperable single-channel radio systems enable coordination with ground troops for close air support and medical evacuation.

SUPPORT TO PORT OPERATIONS

2-121. The theater army G-6 coordinates with the geographic combatant commander to support communications for the harbormaster detachment. The harbormaster detachment coordinates and synchronizes vessel operations. When the detachment arrives, it establishes the satellite communications transport, automated information systems, weather data sensors, and the radio communications necessary to control port operations. Refer to ATP 4-15, for more information about port operations.

BASE CAMP COMMUNICATIONS

2-122. The communications and network support a unit receives in a base camp are similar to the services the network enterprise center provides at their home station. Signal planners determine a base camp's communications requirements based on its size, level of capabilities, and purpose. Tenant and transient units determine their signal requirements based on their operational needs.

2-123. When a G-6 (S-6) or signal unit supports a base camp, the G-6 (S-6) coordinates with the base camp commander to identify communications requirements, including local area network and wide-area network support, DISN services, communications-electronics maintenance, and communications augmentation, as necessary. Refer to ATP 3-37.10 for more information about base camp support.

DEFENSE SUPPORT OF CIVIL AUTHORITIES AND HOMELAND DEFENSE

2-124. The unique capabilities of Army signal systems enable expeditionary signal units to rapidly deploy to support various other contingency or crisis mission requirements. Military communications systems include joint interoperability as a design consideration. However, most communications systems developed for combat are incompatible with civilian systems, unless the military provides specialized connections.

2-125. Signal elements may need to interconnect with various military and commercial communications systems. Compatibility issues may limit the availability of secure communications. The use of disparate communications systems among mission partners introduces additional planning requirements for defense support of civil authorities and homeland defense missions.

2-126. Differing systems, use of allocated civilian and military bandwidth, and limited interoperability complicate collaborative incident management. Signal elements supporting defense support of civil authorities and homeland defense missions collaborate and interoperate with joint and interorganizational partners. These partners include other Military Services and Departments, state and Federal Government agencies, local authorities, and non-governmental organizations.

Defense Support of Civil Authorities

2-127. Army support of civil authorities is a vital aspect of the Army's service to the Nation and a way it maintains trust with citizens (ADP 3-28). The skills that allow Soldiers to accomplish their missions on battlefields can support local, state, tribal, and federal civil authorities, especially when domestic emergencies overwhelm the ability of local government agencies to respond adequately. During defense support of civil authorities, the DOD serves in a supporting role to the Federal Emergency Management Agency and other federal agencies.

2-128. Because not all mission partners can access the DODIN, signal elements tasked for these missions need to interoperate with commercial communications systems. The DODIN-A and DOD gateway can provide connections to the commercial Internet and commercial telephone service for collaboration with non-DOD mission partners.

2-129. Army National Guard units activated under state control (state active duty or Title 32) operate under a separate chain of command from active duty task forces and National Guard troops under federal control (Title 10). Communications interoperability between these forces enables better coordination between the separate chains of command.

2-130. Local communications infrastructure may be inoperable or unreliable after a natural or man-made disaster. The lack of land-based and wireless communications hampers emergency management and first responder operations. Signal units routinely deploy to provide communications and DISN services in austere environments. The same expeditionary capabilities are ideally suited to establishing emergency communications in areas with damaged infrastructure. Because these units have organic power generation equipment, they can establish communications before the commercial power grid is restored, though they need fuel and other logistical support. Expeditionary signal units can provide—

- Emergency restoral of first responder communications.
- Command post communications—voice, data, and video teleconferencing.
- Network connectivity to disseminate the common operational picture.
- Communications to coordinate logistical support.
- Connection to civilian communications infrastructure to interoperate with emergency responders and nongovernmental organizations.
- Communications to areas outside the disaster zone.

Homeland Defense

2-131. The DOD is the primary federal agency for homeland defense. The strategy for homeland defense protects U.S. territory against attack by state and non-state actors through an active, layered defense. This strategy aims to deter and defeat aggression abroad while protecting the homeland. The Army supports this strategy with capabilities in the forward regions of the world, in the geographic approaches to U.S. territory, and within the U.S. homeland. Army signal elements may provide communications to support missions protecting U.S. sovereignty, territory, domestic population, and critical defense infrastructure against external aggression or other threats, as directed by the President.

2-132. Strategic signal capabilities contribute to the United States' day-to-day defensive posture by supporting attack warning and assessment, enabling situational understanding, and helping secure the

cyberspace domain. Both fixed station and expeditionary signal capabilities enable homeland defense operations in the land, air, maritime, space, and cyberspace domains.

2-133. During a homeland defense operation, civil authorities continue to operate and perform many of their routine functions. While homeland security activities of some interagency partners sometimes overlap with homeland defense activities, major military activities are the responsibility of the DOD. Interagency mission partners cannot perform these activities, but their support is essential for mission success.

2-134. Unity of effort among all homeland defense participants is fundamental and essential (JP 3-27). For this reason, homeland defense operations in the United States often require connections to the civilian communications infrastructure to interoperate with various state and federal agencies and nongovernmental organizations. Planners consider joint and interorganizational interoperability as early as possible in the planning process.

Note. The Department of Homeland Security is the lead federal agency for security and defense of civilian U.S. Government cyberspace within the United States.

SIGNAL-ENABLING COMMANDS AND STAFFS

2-135. Signal-enabling commands and staffs support the DODIN-A as a global enterprise network. These entities develop signal capabilities, establish policy and guidance, perform DODIN operations, provide strategic infrastructure, and secure the DODIN-A. These commands, staffs, and agencies support the strategic support area, extend the network to tactical units, and preserve the Army's ability to operate in cyberspace.

CHIEF INFORMATION OFFICER/G-6

2-136. The Chief Information Officer (CIO)/G-6 is the principal staff assistant and advisor to the Secretary of the Army for information management, information technology, and their effects on warfighting capabilities. The CIO/G-6 is also the force modernization proponent for information management (AR 5-22).

2-137. The CIO/G-6 establishes policy for Army use of information technology systems and networks. This responsibility includes evaluating existing Army information management and information technology policies and overseeing their implementation. The CIO/G-6 sets the strategic direction for, and supervises the execution of, Army information management programs and policy. These programs and policies include network architecture, information sharing policy, cybersecurity policy, the Army cybersecurity program, resource management, process modernization, and synchronization of the Army's network activities. The CIO/G-6 exercises Headquarters, Department of the Army oversight to ensure compliance with federal statutes for information technology reform (The Clinger-Cohen Act).

UNITED STATES ARMY CYBER COMMAND

2-138. ARCYBER is the Army Service component command to United States Cyber Command. ARCYBER is the primary Army headquarters responsible for cyberspace operations to support joint requirements. ARCYBER is the single point of contact for reporting and assessing cyberspace incidents, events, and operations in Army networks and for synchronizing and integrating Army responses. When directed, ARCYBER conducts offensive and defensive cyberspace operations to support other Army operations, ensure U.S. and allied freedom of action in cyberspace, and deny the same to adversaries and enemies. ARCYBER provides appropriate-level interactions both as a supported and as a supporting commander to Army commands, other Army Service component commands (including theater armies), direct reporting units, and joint, interorganizational, and multinational elements.

Army Cyber Operations and Integration Center

2-139. The Army Cyber Operations and Integration Center is an operational element of the ARCYBER headquarters. It is the top-level control center for Army cyberspace activities. The Army Cyber Operations and Integration Center provides situational understanding for Army networks and situational awareness of the wider DODIN. The Army Cyber Operations and Integration Center also provides worldwide operational

and technical support across the strategic, operational, and tactical levels, in coordination with the theater armies. The Army Cyber Operations and Integration Center directs the regional cyber centers through operational channels. The Army Cyber Operations and Integration Center interfaces with the functional network operations and security centers, and coordinates with other Service and agency DODIN operations centers, through technical channels.

2-140. The Army Cyber Operations and Integration Center analyzes threat information and directs network security actions through the regional cyber centers, in coordination with the theater armies. The Army Cyber Operations and Integration Center develops technical solutions to secure Army networks and helps Army units and regional cyber centers implement cybersecurity policy. Refer to ATP 6-02.71 for more information about the Army Cyber Operations and Integration Center.

United States Army Network Enterprise Technology Command

2-141. United States Army Network Enterprise Technology Command (NETCOM) is the Army's global enterprise network service provider. NETCOM is subordinate to ARCYBER, provides global DODIN operations oversight, and performs inter-theater DODIN operations functions to ensure interoperability across the DODIN-A. NETCOM enforces Army-wide standards established by the CIO/G-6 to preserve joint, interorganizational, and multinational interoperability.

2-142. NETCOM integrates Army information technology to achieve a single, virtual enterprise network. NETCOM enforces service delivery activities, cybersecurity policies, processes, procedures, and protocols for operation of Army networks. To ensure unity of effort in DODIN operations, NETCOM has direct liaison authority to the CIO/G-6, with notification to ARCYBER.

2-143. NETCOM manages the DODIN-A, including enforcing technical standards, and configuration management. NETCOM is the single entry point to submit validated, approved telecommunications requirements for coordination and implementation by the Defense Information Systems Agency.

2-144. NETCOM manages the administration of amateur radio operations and the Army Military Auxiliary Radio System program pursuant to AR 25-6 and provides COMCAM support for theater army and joint military operations. NETCOM manages and services spectrum-related requirements for Army installations in accordance with U.S., DOD, Army, host-nation, and international spectrum regulations, policies, and technical standards.

Signal Command (Theater)

2-145. The SC(T) is a subordinate command of NETCOM which provides oversight, leadership, and technical direction over the theater network. The SC(T) provides DODIN operations and spectrum management support across the theater. The SC(T) provides these capabilities—

- Centralized management of Army data, voice, and video networks, including interfaces with joint, interorganizational, and multinational systems in the theater.
- Enforcement of global cybersecurity policies to support the geographic combatant commander and theater army commander.
- Oversight of units building, configuring, securing, operating, and maintaining signal support systems and network interfaces to joint and multinational partner systems in theater.
- Establishment of mission priorities to ensure DODIN-A capabilities are available to meet commanders' information requirements.

Regional Cyber Center

2-146. The regional cyber center is the single point of contact for Army network services, operational status, service provisioning, service interruption resolution, and service restoral in its operational area. The regional cyber center is responsible for intra-theater communications, with a focus on tactical communications support. The regional cyber center supports the strategic network by providing DODIN operations oversight for up to eight network enterprise centers. The regional cyber center provides network status information to the Defense Information Systems Agency's enterprise operations center and the Army Cyber Operations and Integration Center. The regional cyber center may also provide network status to other Service component

DODIN operations centers to enable shared situational understanding. The regional cyber centers perform the same functions in all theaters.

2-147. The regional cyber centers' operational areas and core missions align with the theater and field army commanders' operational areas:

- United States Army Regional Cyber Center-CONUS (continental United States and South).
- United States Army Regional Cyber Center-Europe (Europe and Africa).
- United States Army Regional Cyber Center-Korea.
- United States Army Regional Cyber Center-Pacific.
- United States Army Regional Cyber Center-Southwest Asia.

2-148. The regional cyber center performs or coordinates DODIN operations tasks that span the theater or multiple theaters. Centralizing high-level tasks provides consistent service among regions by performing the operational function at the only location with visibility or awareness of multiple regions.

2-149. The regional cyber center is under operational control of the Army Cyber Operations and Integration Center directs for DODIN operations, defensive cyberspace operations-internal defensive measures, network vulnerability assessment, and incident management within the theater. The regional cyber center collaborates with the Army Cyber Operations and Integration Center to—

- Coordinate threat assessments and support to multi-agency vulnerability assessments with the supporting counterintelligence element.
- Develop countermeasures and defensive cyberspace operations strategies.
- Conduct attack signature sensing and warning analysis.
- Develop mitigation strategies to support network defense and prevent data loss, including spillage. *Spillage* is a security incident that results in the transfer of classified information onto an information system not authorized to store or process that information (CNSSI 4009). An example of spillage is SECRET data on NIPRNET.
- Conduct the computer defense assistance program to support commanders in theater. The computer defense assistance program includes penetration testing, network assistance visits, and network damage assessments.

Tactical Actions Center

2-150. The NETCOM tactical actions center provides enterprise network engineering, planning, operations, and cybersecurity support within a theater of operations that has no assigned SC(T). The tactical actions center provides strategic and tactical planning, operations, and cybersecurity support to meet inter-theater communications requirements. The tactical actions center is the in-theater lead for planning, engineering, and executing NETCOM projects and operations.

Strategic Signal Brigade

2-151. Strategic signal brigades provide operational and strategic support area signal support to serve warfighters in a theater of operations. This support includes long-haul transport, communications infrastructure, automation, and network management. The strategic signal brigade provides—

- Operational direction through technical channels to the network enterprise center in provisioning services.
- Access to the DODIN-A for fixed station Army assets within its theater.
- Gateway access to the DODIN-A for expeditionary Army units.
- Advice to commanders, staff, and users on the capabilities, limitations, and employment of communications, network, and automated information system assets.
- Advice to supported commanders and staff on information management, automation policy, technical matters, and system performance.
- Input to all-source intelligence assessments and estimates concerning the DODIN-A at the operational and strategic levels.

2-152. Outside the continental United States, the strategic signal brigade provides communications planning and command and control for an assigned expeditionary signal battalion. This allows the strategic signal brigade to meet contingency and emerging tactical communications support requirements in theater without going through the lengthy request for forces process.

Strategic Signal Battalion

2-153. Strategic signal battalions are regionally based signal elements. They manage communications infrastructure in their geographical areas and configure, secure, operate, and maintain network facilities to support strategic signal brigade, SC(T), and NETCOM missions. The battalion headquarters supports the unit's mission through—

- Staff planning and operational supervision of assigned companies and teams.
- Supervision of signal support, communications, automation, and visual information.
- Planning, engineering, and technical control of strategic communications systems.

2-154. The strategic signal battalions' equipment and personnel authorizations support unique mission sets, based on the battalion's location and function. Most of their subordinate elements operate and maintain equipment at fixed locations. The capabilities a strategic signal battalion may provide include—

- Long-haul, inter-theater satellite communications transport.
- Regional hub node to extend DISN services to deployed expeditionary units.
- Fixed station microwave transport.
- Technical control facilities.
- Geographic combatant commander communications support.
- Data centers.
- Installation-level DODIN operations (network enterprise center).
- Connectivity to DISN services, including NIPRNET, SIPRNET, Defense Red Switched Network, Defense Switched Network, Organizational Messaging Service, video teleconferencing, and local telephone exchange services (network enterprise center).
- COMSEC material issue and management.
- COMSEC equipment maintenance.
- Installation and maintenance of copper and fiber optic cable systems and related equipment.

Expeditionary Signal Battalion (Theater-Committed)

2-155. Some strategic signal brigades outside the continental United States also have an expeditionary signal battalion assigned so they can support the entire range of military operations. These battalions and their companies are theater-committed, not part of the global rotational force pool. A theater-committed expeditionary signal battalion has the same capabilities and functions as a rotational unit, but it usually supports only its assigned theater. See paragraph 2-58 for detailed capabilities of an expeditionary signal battalion.

Network Enterprise Center

2-156. The network enterprise center provides overall DODIN operations, and is responsible for information management, information technology management, and telecommunications services on its post, camp, or station, or within its designated service area. Network enterprise centers coordinate, plan, program, and execute electromagnetic spectrum management on their installation (ATP 6-02.70). Network enterprise centers collaborate with external organizations to ensure proper operation of the installation-level components of DOD or Army networks and information systems. The network enterprise center's DODIN operations responsibilities include—

- Managing support functions for customer access to the installation network and information systems infrastructure.
- Coordinating support and problem resolution for physical networks and information technology equipment on the installation, or within the network enterprise center's designated service area.
- Representing supported units in recommending changes to the DODIN, based on lessons and best practices.
- Implementing DOD and industry best practices, according to DOD, Army, and SC(T) guidance.
- Establishing local policies and procedures for networks and information systems within its service area.
- Establishing individualized service level support agreements between tenant units and the SC(T).
- Coordinating with the strategic signal battalion to manage inter-installation networks affecting supported organizations.
- Managing the installation cybersecurity program.
- Managing the activities, functions, and capabilities of the network and information systems resources within its service area, according to direction from the SC(T) and regional cyber center.
- Assessing the mission impact of outages, DODIN operations incidents, and other network issues and reporting to the regional cyber center.

UNITED STATES ARMY COMMUNICATIONS-ELECTRONICS COMMAND

2-157. United States Army Communications-Electronics Command provides worldwide life cycle sustainment and equipment readiness support. The command also provides training support and on-site logistics assistance to units at their home stations inside and outside the continental United States and deployed units.

Sustainment Maintenance Support

2-158. United States Army Communications-Electronics Command provides sustainment maintenance for communications-electronics systems. Sustainment maintenance consists of depot maintenance and below depot maintenance. See appendix C for more information about depot and below depot sustainment maintenance.

Communications Security Support

2-159. The Communications Security Logistics Activity is the Army commodity manager for COMSEC materiel. The Communications Security Logistics Activity acquires, distributes, and provides logistical support for COMSEC equipment, cryptographic keying material, and other encryption products for Army users.

UNITED STATES ARMY SPACE AND MISSILE DEFENSE COMMAND/ARMY FORCES STRATEGIC COMMAND

2-160. United States Army Space and Missile Defense Command/Army Forces Strategic Command engineers, operates, and provides technical expertise for its assigned satellite systems, including Wideband Global Satellite Communications. The United States Army Space and Missile Defense Command/Army Forces Strategic Command G-6 is the designated DOD satellite communications systems expert for—

- Wideband satellite communications.
- Narrowband satellite communications.
- Wideband Global Satellite Communications.
- Defense Satellite Communications System.
- Global Broadcast Service.
- Mobile User Objective System.

Regional Satellite Communications Support Center

2-161. United States Army Space and Missile Defense Command/Army Forces Strategic Command operates the regional satellite communications support centers. The regional satellite communications support centers are geographically distributed, multi-Service organizations. The regional satellite communications support centers provide planning, engineering, and satellite payload management for all military satellite communications systems. The regional satellite communications support centers' staffing includes personnel from the Army, Navy, Air Force, and the Defense Information Systems Agency.

2-162. The regional satellite communications support centers provide 24-hour satellite communications resources, systems engineering, and modeling support. The regional satellite communications support centers analyze requirements and develop solutions to support users in day-to-day management of satellite communications resources allocated for the combatant command. They also process satellite access requests to authorize the use of space and ground terminal resources via satellite access authorizations.

Signal Battalion (Satellite Control)

2-163. The signal battalion (satellite control) manages satellite communications networks and controls communications payloads on the Defense Satellite Communications System and Wideband Global Satellite Communications constellations. Signal Soldiers with specialized satellite network control training perform these missions. These centers enable satellite communications support for the President, Secretary of Defense, Chairman of the Joint Chiefs of Staff, Military Services, the Department of State, intelligence activities, combatant commanders, and selected allied forces during unified action.

2-164. The wideband satellite communications operations centers support Army operations by—

- Monitoring and controlling use of Defense Satellite Communications System and Wideband Global Satellite Communications satellites networks.
  - Satellite link establishment.
  - Satellite link quality monitoring and maintenance.
  - Satellite link power management.
  - Satellite communications earth terminal monitoring.
  - Terminal positive control and subnetwork control.
- Transmission and communications payload control of assigned Defense Satellite Communications System and Wideband Global Satellite Communications satellites.
  - Payload command and telemetry.
  - Electromagnetic interference detection and geolocation.

2-165. Refer to FM 3-14 for more information about Army space operations. Refer to ATP 6-02.54 for more information about the satellite control battalion and regional satellite communications support centers.

SECTION II – CORE COMPETENCIES AND ESSENTIAL CAPABILITY OF THE SIGNAL CORPS

DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS

2-166. In the past, the Army and DOD have treated network operations as a task performed to manage the network. DODIN operations are not an individual or crew task, but multifaceted military operations that take place at all echelons. DODIN operations are arguably the most important and most complex operation the Army performs from day-to-day, since the network is the foundation for all other functions and capabilities, including command and control; joint intelligence, surveillance, and reconnaissance; precision fires; logistics; and telemedicine.

2-167. DODIN operations support both the generating and operational forces. DODIN operations ensure system and network availability, information protection, and information delivery to maintain freedom of

action in cyberspace. Because they are so complex and have such wide-ranging impact on the information environment, DODIN operations require deliberate planning through the military decision-making process and coordinated execution through the operations process.

2-168. Effective DODIN operations make network-enabled operations possible. DODIN operations are a commander-focused activity. Signal staffs prepare DODIN operations plans and courses of action and commanders make the decisions. DODIN operations technical channels parallel the operational chain of command to maintain unity of command and unity of effort. This allows commanders to align available communications and network support to their highest mission priorities.

DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS TASKS

2-169. Achieving information superiority requires unity of effort in command, control, and management of the DODIN. As a practical matter, unity of effort is necessary due to the vast number of information technology resources required to support worldwide DODIN operations (JP 6-0). DODIN operations functions ensure availability and security of information technology resources and services and the information they provide.

2-170. Each of the Military Services performs DODIN operations to DOD-wide standards to ensure joint interoperability. Signal Soldiers control, secure, and manage the flow of information over DOD networks through DODIN operations. DODIN operations tasks are active measures implemented across the entire DODIN. Joint DODIN operations involve the employment of these essential joint tasks:

- **DODIN enterprise management** is the technology, processes, and policies necessary to engineer, install, operate, maintain, and sustain DOD communications networks, information systems, and applications. Enterprise management merges information technology services with the DODIN operations capabilities.
- ***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). Cybersecurity policies are not specific to a threat actor. They establish the baseline security posture of the network and mitigate risks associated with known exploits and vulnerabilities to DOD information systems and computer networks. Cybersecurity provides the ability to monitor for, detect, and analyze unauthorized activity within DOD information systems and computer networks.
- **DODIN content management** allows DODIN operations centers to optimize the flow and location of information over the DODIN by positioning and repositioning data and information services to optimum locations on the network relative to the information producers, information consumers, and mission requirements.

2-171. Shared network status across the DODIN is critical to situational understanding and decision making. Shared situational awareness and coordination between stakeholders on network events helps commanders and non-information technology staff understand the impact of DODIN operations on the information environment and the operational mission. Network situational awareness identifies cybersecurity policy violations and aids in network troubleshooting and restoral. Unusual network activity might provide the first indication of a cyberspace attack. Comprehensive network situational understanding, combined with current intelligence estimates, allows the CEMA section to synchronize signal capabilities with cyberspace and EW operations.

2-172. DODIN operations require centralized coordination because they have the potential to impact the integrity and operational readiness of the DODIN; however, execution is generally decentralized (JP 6-0). The Army conducts DODIN operations within the DODIN-A and in other DOD networks, as required. For this manual, the term DODIN operations refers to these activities on any DOD network.

DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS IN ARMY NETWORKS

2-173. DODIN operations provide integrated network visibility and end-to-end management of networks, applications, and services across the DODIN-A. Network visibility enables commanders to control and exercise command authority over their networks as they would other warfighting platforms.

2-174. DODIN operations personnel operate and secure the network to achieve information advantage supporting Army and joint missions. Unlike many missions considered successful at a defined completion date, DODIN operations are ongoing. The mission requires continuous support to achieve success.

2-175. DODIN operations allow commanders to employ network-enabled capabilities to shape and influence their areas of operations. For the Army, DODIN operations consists of three essential tasks:

- **Network management and enterprise systems management**—install, operate, and maintain Army communications and computer networks, systems, and applications to achieve information advantage. Network management provides networked services with the desired quality and availability. Enterprise systems management provides day-to-day management of information systems, elements of systems, and services, including operating systems, databases, and end-user systems. Network management and enterprise systems management correspond to, and nest within, the joint task of DODIN enterprise management.
- **Cybersecurity**—provides end-to-end protection to ensure data confidentiality, integrity, and availability, as well as protection against unauthorized access. The cybersecurity functions are—identify, protect, detect, respond, and recover. Organizations manage cybersecurity risk by organizing information, implementing the risk management framework, addressing vulnerabilities, and improving security by learning from past activities. Cybersecurity in the DODIN-A is the same as cybersecurity across the wider DODIN.
- **Information dissemination management and content staging**—emplace, manage, provide, and restore information services to enable information and knowledge management. Information dissemination management supports effective knowledge management so the right information reaches the right users at the right time, in a usable format. Content staging compiles, catalogs, and caches information. The Army task of information dissemination management and content staging corresponds to, and nests within, the joint task of DODIN content management. Information dissemination management and content staging consist of the technologies, techniques, processes, policies, and procedures to provide warfighters—
  - Awareness of relevant, accurate information.
  - Automated access to newly revealed or recurring information.
  - Timely, efficient, delivery of information in a usable format.
  - The DODIN operations essential tasks take place at the strategic, operational, and tactical levels and support all warfighting and business functions. DODIN operations enable network and system availability, information protection, and timely information delivery across strategic, operational, and tactical boundaries.
  - Network and information system availability. Ensuring availability of system and network resources. This includes providing for continued operation in a degraded environment, self-healing, and eliminating critical failure points.
  - Information delivery. Providing required information to users, planners, and decision makers. DODIN operations personnel continuously monitor the network to ensure information transfer is timely and network throughput and performance meet user requirements.

2-176. Figure 2-2 on page 2-34 shows the DODIN operations critical tasks with their individual and combined effects. Network management and enterprise systems management (DODIN enterprise management) consist of steps to configure, allocate, process, connect, route, flow, account for, and maintain network capabilities. Information dissemination management and content staging (DODIN content management) allow users to retrieve, cache, compile, catalog, and distribute information to support planning and decision making. Cybersecurity provides the means to resist and recognize intrusions and to recover and reconstitute network capabilities. The net effect of integrating the three tasks is information advantage. Users get timely, protected information to meet their critical information requirements. Refer to ATP 6-02.71 for more information about DODIN operations in Army networks.

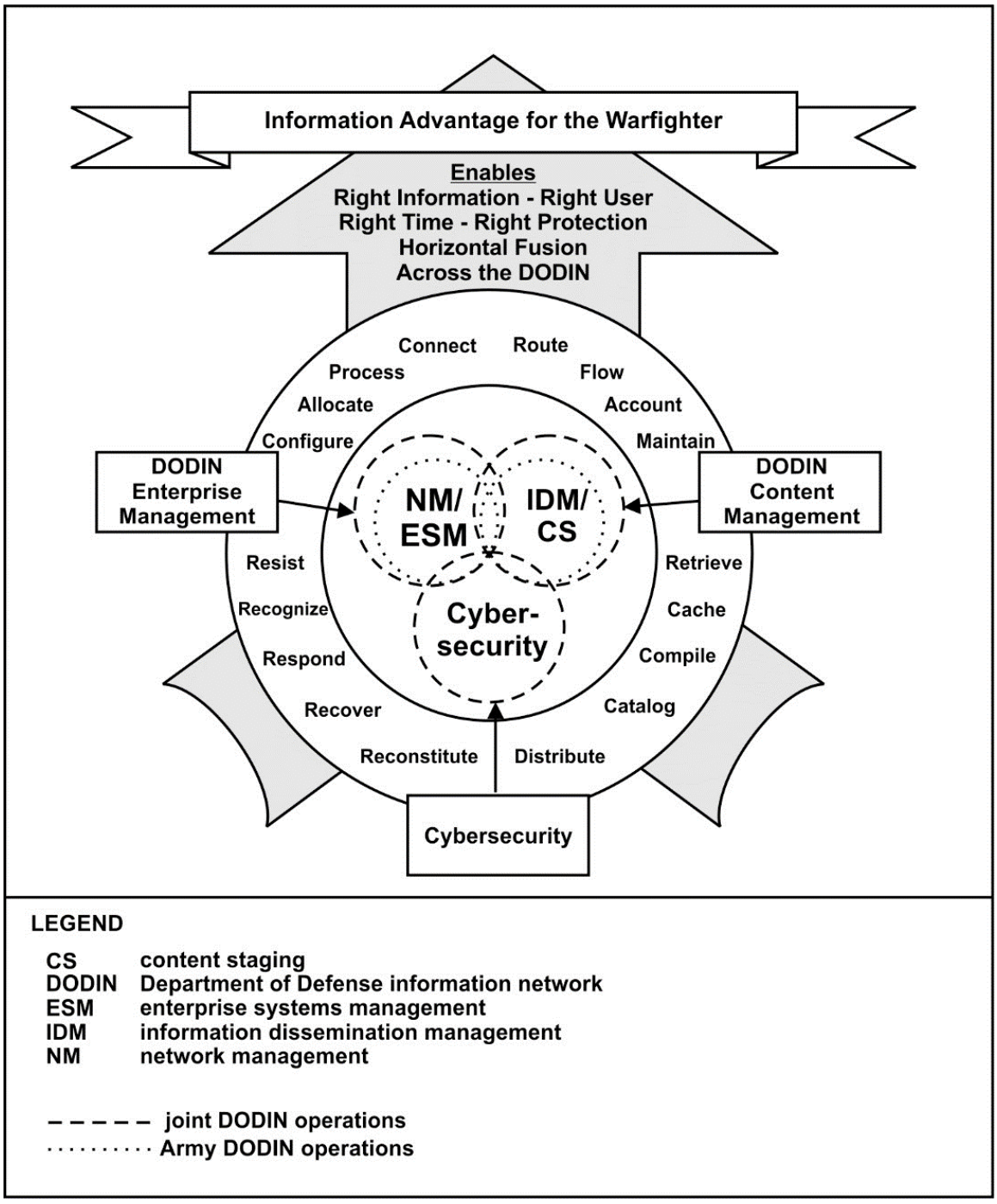


Figure 2-2. Department of Defense information network operations components, effects, and objectives

NETWORK TRANSPORT AND INFORMATION SERVICES

2-177. Network transport and information services encompass the combined physical assets and activities to ensure data reliably transverses the network. ***Network transport*** **is the processes, equipment, and transmission media that provide connectivity and move data between networking devices and facilities.** Information services enable planning, controlling, and manipulating information throughout its life cycle.

2-178. Network transport and information services connect users, automated information systems, and applications throughout the Army enterprise. Network transport connects networking hardware and carries data over distance to integrate local area networks and wide-area networks into the DODIN-A. Information services provide computing and networking capabilities to facilitate human interaction, staff integration, and interoperability with mission partners. When combined, network transport and information services enable the flow of data and information among applications, systems, and users.

2-179. The network connects geographically separated forces for network-enabled operations. By integrating information from across the operational area, Army forces can maintain more complete, relevant situational understanding. The integrated common operational picture allows commanders to employ the right capabilities, in the right place, at the right time to meet critical information requirements.

NETWORK TRANSPORT

2-180. Network transport moves data between networking facilities. Globally prepositioned network transport capabilities extend access to DISN services worldwide to support Army operations.

2-181. The long-haul transport is the fixed backbone network provided by the Defense Information Systems Agency as part of the DISN interface. The fixed backbone network provides communications infrastructure for permanent installations and DOD Gateways as prepositioned connection points to connect deployed units to the DODIN. Network transport includes all data transmission capabilities that extend DISN access across the strategic, operational, and tactical levels. Key network transport capabilities are—

- Satellite communications.
- Line of sight and troposcatter systems.
- Tactical radios and radio retransmission.
- Copper wire and cable.
- Fiber optics.

2-182. Network transport connects elements across all echelons, so the DODIN-A can operate as an integrated network. The network transport resources to connect the clients can belong to U.S. or non-U.S. forces, host nations, or commercial entities. Adequate network transport throughput capacity is critical to reliable cloud services, reachback, and the shift from locally-provided to enterprise services. Refer to ATP 6-02.54 for more information about satellite communications transport. Refer to ATP 6-02.53 for more information about tactical radios and radio retransmission.

INFORMATION SERVICES

2-183. Information services allow access, storage, and sharing of information among mission partners, as well as dynamically tailoring and prioritizing information to support the mission and affect the operational environment. Information services allow commanders and Soldiers to collect, process, store, transmit, display, and disseminate information. Information services consist of—

- **Messaging services** enable warfighters to exchange information among users. Messaging services include e-mail, Organizational Messaging Service, instant messaging, and alerts.
- **Discovery services** enable warfighters to discover information content or services stored in directories, registries, and catalogs. An example of a discovery service is a search engine.
- **Mediation services** enable system interoperability by processing data to translate, aggregate, fuse, or integrate it with other data.
- **Collaboration services** provide the ability for warfighters to work together and share capabilities. Examples of collaboration services are chat, online meetings, and workgroup applications.
- **Storage services** provide physical and virtual data hosting. Storage services include archiving, continuity of operations, and content staging. Standard operating procedures or operation orders should define information storage locations.
- **User assistance services** provide centralized service desk assistance and automated access to lessons and best practices, which may improve processes or reduce the effort required to perform tasks.

- **Identity and access management** (Enterprise Directory Service) provides authoritative enterprise identity and contact attributes for combatant commands, Services, and agencies. Enterprise Directory Service includes—
- **DOD Enterprise White Pages**—authoritative identity and contact information for all DOD common access card holders.
- **Global Directory Service**—a distribution point for personal public key certificates, certificate revocation lists, and certificate authority certificates.
- **Identity Synchronization Service**—populates directories and global address lists with enterprise identity and contact attributes.

2-184. These services also support joint, interorganizational, and multinational collaboration. Information sharing allows the mutual use of information services or capabilities across functional or organizational boundaries.

2-185. Identity and access management services facilitate and control information sharing. Identity and access management assigns users common, portable identity credentials, such as a common access card or SIPRNET token. Users with the proper credentials can access and view operational, business support, or intelligence-related information, services, and applications related to their mission and communities of interest. Refer to ATP 6-02.71 for more information about information services.

SPECTRUM MANAGEMENT OPERATIONS

2-186. Since a significant part of any communications system relies upon wireless transmissions, communications planners must consider access to the electromagnetic spectrum. Signal Soldiers support assured access through spectrum management operations. ***Spectrum management operations*** **are the interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations.** Spectrum management operations enable access to the frequency spectrum to support Army operations.

2-187. Spectrum management includes operational, engineering, and administrative procedures to plan, coordinate, and manage use of the electromagnetic spectrum. Spectrum managers prioritize and deconflict operation of spectrum-dependent systems to prevent unacceptable interference. They may coordinate spectrum use with U.S. or host-nation military and civil authorities. Spectrum management includes enforcing frequency assignments while identifying and eliminating unauthorized use of the frequency spectrum.

2-188. Frequency assignment involves requesting and issuing authorization to use frequencies for specific equipment. This includes assigning frequencies for combat net radio networks, unmanned aircraft systems, and line of sight networks. Spectrum managers perform frequency assignment for all spectrum-dependent military equipment.

2-189. Host nation coordination is negotiation for authorization to operate radio frequency-emitting equipment within a sovereign nation. This coordination is necessary to conform to international and national laws, and to avoid interfering with host-nation communications and emergency services. Coordination prevents diplomatic friction with the host nation. Commanders or operators who do not operate within host-nation laws may incur criminal or civil liability and have their equipment confiscated. Host nation coordination does not apply to forcible entry operations or operations in a hostile nation.

2-190. Spectrum management operations depend on policy adherence to ensure access to the spectrum. This includes complying with national (strategic) through tactical-level policies and defining local policies for spectrum management, frequency assignment, and host nation coordination. Refer to JP 6-01 and ATP 6-02.70 for more information about spectrum management.

VISUAL INFORMATION AND COMBAT CAMERA

2-191. Visual information and COMCAM capture still and motion imagery to support a variety of missions. Visual information products may support command and control, training, education, logistics, human

resources, special operations, information operations, public affairs, or intelligence requirements. Visual information and COMCAM provide decision makers and supported agencies current and accurate information.

VISUAL INFORMATION

2-192. *Visual information* is various visual media with or without sound that generally includes still and motion photography, audio video recording, graphic arts, and visual presentations (JP 3-61). Visual information also includes the activities to produce and edit these products.

2-193. Unlike news stories, press releases, or press conferences, Army visual information records events as they occur. It documents military operations, exercises, and activities to convey an unfiltered view to key audiences. Visual information products are subject to the same security classification and operations security considerations as other operational information.

2-194. Visual information products created for other uses can also support public affairs objectives. Multi-use examples of visual information include—

- Documenting domestic disasters to aid emergency management decision making.
- Documenting evidence of war crimes.
- Preserving evidence about damage claims against the U.S. Government.
- Providing training aids that simulate battlefield conditions.
- Providing battle damage assessment images.
- Documenting forensic evidence of incidents, such as improvised explosive device detonations.
- Documenting the environmental impact of military operations.

2-195. Visual information support is limited to official events or activities. Commanders consider the mission, cost-effectiveness, and the quality and quantity of products and services available when establishing priorities for visual information support.

2-196. The Defense Imagery Management Operations Center receives, manages, and distributes strategic, operational, tactical, and joint-interest imagery as a shared asset. See appendix C for more information about requests for visual information resources.

2-197. Regardless of the mission and conditions under which visual information is created, it becomes an official DOD record and may be releasable under the Freedom of Information Act, requests for evidence in litigation, or other sources of legal authority (JP 3-61). The release of visual information products is subject to security classification and operations security review. Refer to ATP 6-02.40 for more information about visual information operations.

Note. Certain visual information-type imagery is exempt from mandatory disclosure and sharing. Visual media collected exclusively to support intelligence, law enforcement, medical, or research, development, test, and engineering activities, and imagery from weapon systems, helmet cameras, or unmanned aerial vehicles fall under separate regulatory guidance. Refer to DODI 5040.02 for more information on these exclusions.

COMBAT CAMERA

2-198. *Combat camera* is specially-trained expeditionary forces from Service-designated units capable of providing high-quality directed visual information during military operations (JP 3-61). COMCAM units and teams produce still and motion imagery to support combat, information operations, humanitarian relief, special operations, intelligence, reconnaissance, engineering, legal, public affairs, and other operations involving the Military Services. COMCAM is an essential battlefield information resource that supports strategic, operational, and tactical mission objectives.

2-199. Commanders employ COMCAM capabilities to document the entire scope of U.S. military activities during wartime operations, crises, contingencies, joint exercises, and other events of significant national interest involving the DOD Components. The COMCAM mission may support, but is separate from,

specialized imagery operations and systems for specific mission requirements, such as intelligence, surveillance, and reconnaissance or operational test and evaluation.

2-200. COMCAM supports Army units across the range of military operations. COMCAM elements share documentation, as required, to support operational and planning requirements from tactical through national level. COMCAM documentation supports sound decision making. COMCAM capabilities include—

- Tactical digital media.
- Imagery editing.
- Video editing.
- Transmission of visual information products.
- High definition still and video imagery.
- Graphic design.
- Parachute-qualified COMCAM equipped Soldiers (airborne COMCAM company only).

2-201. COMCAM requirements are different from public affairs and press pool media requirements. While COMCAM imagery may support public affairs, it is primarily a decision-making tool. Because COMCAM Soldiers can access information and areas media personnel cannot, the imagery they produce is often operationally sensitive. COMCAM imagery requires security classification and operations security review before release for public affairs use. See appendix C for COMCAM request procedures. Refer to ATP 6-02.40 for more information about COMCAM.

COMMUNICATIONS SECURITY

A strong case can be made that, seen broadly, a major purpose of COMSEC—perhaps its overriding purpose—is to help achieve surprise by denying adversaries and enemies foreknowledge of our capabilities and intentions."

David G. Boak

2-202. Communication is more than the simple transmission of information. It is a means to exercise control over forces. Communication links information to decisions and decisions to action. Communication among the parts of a command supports their coordinated action (ADP 6-0). Operations security concerns dictate that U.S. forces deny adversaries and enemies the content of sensitive communications.

2-203. *Communications security* is the protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study (JP 6-0). While COMSEC does not rise to the level of a core competency, it is still an essential capability to protect sensitive information.

2-204. Cryptographic systems and devices protect sensitive classified and unclassified operational information in the DODIN-A. To decrypt the data, every member of the cryptonet needs an identical key. COMSEC account managers distribute and control keying material and manage routine updates so all authorized users—and only authorized users—have the correct key to communicate. Including COMSEC key management in operations planning is essential to enabling secure communications.

2-205. If cryptographic equipment or keying materials become lost or captured, the communications they secure risk compromise. This is especially true of a keyed device, such as a combat net radio, since a lost or captured radio compromises the entire network. Promptly reporting a lost key facilitates risk assessment and mitigation. Refer to ATP 5-19 for more information on risk management.

2-206. Normally, when a cryptographic key is lost, the controlling authority initiates emergency key supersession to protect the integrity of the cryptographic network. Any member of the cryptonet who does not have the new key, will lose communications over the network until they obtain and update their key. If mission requirements prevent immediate supersession, the key update should take place as soon as the mission allows. The commander's risk decision must consider the likelihood the keying material has fallen into enemy hands.

2-207. COMSEC account managers maintain centralized accountability of cryptographic material and equipment. For tactical flexibility, operators and COMSEC local elements hold keying material and devices at the lowest echelon that can maintain appropriate physical security. This allows COMSEC managers and operators to react to contingencies, such as emergency key supersession, equipment failure, or operator error with minimal downtime.

2-208. COMSEC compliance is a command responsibility. Users are responsible for protecting and accounting for all COMSEC material and equipment in their possession or control. TB 380-40 provides further guidance on COMSEC responsibilities. Refer to ATP 6-02.75 for more information about COMSEC operations.

SECTION III – SIGNAL TRAINING

INDIVIDUAL SIGNAL TRAINING

2-209. The United States Army Signal School conducts training, leader development, and continuing education. The Signal School conducts both resident training at the Cyber Center of Excellence, and sustainment training at the cyber learning centers.

RESIDENT TRAINING

2-210. The Signal school trains officers, warrant officers, and enlisted Soldiers in signal branch designations, functional areas, and military occupational specialties. This responsibility includes—

- Signal branch officer basic and career courses.
- Functional area 26A and 26B transition courses.
- Warrant officer courses.
- Advanced individual training.
- Enlisted military occupational specialty reclassification.
- Noncommissioned officer education system courses.
- Functional courses, such as signal digital master gunner and COMSEC account manager.

2-211. Signal Soldiers receive training to—

- Plan and direct signal support.
- Provide network transport and information services, including automated information systems integration.
- Operate telecommunications systems and networks.
- Secure the confidentiality, integrity, and availability of telecommunications networks, automated information systems, and data (cybersecurity).
- Conduct spectrum management.
- Manage COMSEC.
- Conduct visual information and COMCAM operations.

SUSTAINMENT TRAINING

2-212. The regional signal training sites—formerly United States Army Communications-Electronics Command signal and sustainment universities—serve Active Component units at many installations. The cyber learning centers are a key training capability for emerging technology, communications, information technology applications, and commercial certifications. The individual training and certifications available from the cyber learning center support units' training readiness and can be a valuable tool in the unit's overall training plan. For more information about course offerings, contact the installation's cyber learning center.

COLLECTIVE SIGNAL TRAINING IN UNITS

2-213. The Army prepares itself for large-scale combat operations continuously. There is no time to build readiness necessary to win once hostilities commence in the current operational environment. Army forces must demonstrate a credible level of readiness against regional peer threats to effectively deter adversaries and assure partners (FM 3-0).

2-214. Commanders understand a key to mission success is training their Soldiers in the tasks and battle drills required to execute the unit's primary mission. Experience at home station exercises, the combat training centers, warfighter exercises, and deployments shows the importance of allowing enough time in the training schedule for operator and crew training on critical signal support systems. The individual and team tasks to operate and maintain these systems are complex, and the skills are perishable. Without regular training, Soldiers' proficiency quickly degrades. This is especially true for general-purpose user systems not operated by signal Soldiers. Because typical operators are less familiar with signal equipment and concepts, they need regular refresher training with these systems.

2-215. Collective tasks are clearly defined, observable, and measurable activities or actions that require organized team or unit performance, leading to the accomplishment of a mission or function. Based on the accomplishment of task proficiencies at the individual level, units conduct collective training. This is done at home station, at maneuver combat training centers, at mobilization training centers, during joint training exercises, and while deployed (ADP 7-0).

MISSION ESSENTIAL TASKS

2-216. Commanders rarely have enough time or resources to train all tasks. The commander evaluates the unit's task proficiency to determine which essential collective tasks the unit must train to attain the required proficiency and on which tasks they can accept risk. The organic signal company's combined arms training strategy includes a mission essential task list. Each mission-essential task aligns with supporting collective and individual tasks.

COLLECTIVE TRAINING TECHNIQUES

2-217. 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

2-218. The training environment should duplicate as closely as possible the expected operational environment. 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.

2-219. 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.

2-220. 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.

2-221. 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

2-222. Digital battle drills provide signal equipment operators and teams structured, pre-planned responses to network, COMSEC, cybersecurity, or server-related events or power outages. Established standards are easy to enforce and help manage expectations inside the command. Realistic training and repetition ensure operators can reflexively apply conditioned responses under combat conditions. All echelons should formulate and actively rehearse battle drills for a variety of anticipated events to ensure timely and appropriate responses.

Combined Arms Training Strategy

2-223. 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 their assigned systems. As training progresses, teams combine for platoon- and company-level training exercises to ensure the teams can integrate the unit's network systems into the DODIN-A. Training signal teams to proficiency through the combined arms training strategy ensures Soldiers are not only proficient in their individual military occupational specialty skills, but can integrate the network to support operations.

SIGNAL DIGITAL MASTER GUNNER COURSE

2-224. The Signal Digital Master Gunner Course is a functional course that trains signal noncommissioned officers to install, operate, maintain, and secure local area networks and integrate them with mission command information systems and the unit's portion of the DODIN-A. The course teaches Soldiers to integrate commercial server applications with tactical communications systems. Signal digital master gunner is a resident course taught at the Signal School.

SECTION IV – THE ARMY NETWORK

2-225. Army forces depend on the DODIN-A for network-enabled operations throughout all operational phases and environments. This section discusses the joint (DODIN) and Army (DODIN-A) networks, the network transport and information services capabilities that enable command and control, and DODIN operations.

DEPARTMENT OF DEFENSE INFORMATION NETWORK

2-226. The joint force depends upon the DODIN to connect strategic, operational, and tactical commanders across the globe. The DODIN enables the right users to access the right information at the right time to enable situational understanding and timely decision making, with the right protection to prevent disclosure to enemies and adversaries.

2-227. As the DOD portion of cyberspace, the DODIN interacts with and provides connections to national and global cyberspace. The DODIN consists of joint capabilities provided by the Defense Information Systems Agency combined with Service-specific enclaves provided by the Army (DODIN-A), Navy, Air Force, and Marine Corps. An *enclave* is a set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter (CNSSI 4009).

2-228. The DODIN can store user data or make data stores available through commercial cloud service providers. The Defense Information Systems Agency manages DISN applications and services through core data centers in each geographic combatant commander's area of responsibility. The servers at the core data

center provide always-on, secure data storage. This data storage capability enables deploying Soldiers and units to take their home-station information with them whenever and wherever they deploy by transferring the data from their home station data center to the data center serving their deployment area of operations. Core data centers support the DODIN worldwide so users can access Army, joint, and multinational data, applications, and information services from anywhere, at any time, in any operational environment

COMMAND AND CONTROL

2-229. United States Cyber Command has the Unified Command Plan mission to operate, secure, and defend the DODIN. For unity of command and unity of effort, Joint Force Headquarters-DODIN exercises delegated directive authority over all DOD Services and agencies for DODIN operations and defensive cyberspace operations-internal defensive measures. Within the Army, ARCYBER plans and directs cyberspace operations, including DODIN operations.

Note. The Director of the Defense Information Systems Agency is designated as the Commander, Joint Force Headquarters-DODIN.

ARCHITECTURE

2-230. The DODIN architecture identifies priority areas, principles, rules, and activities to implement a manageable set of enterprise-wide capabilities. The architecture provides a common vocabulary for describing the capabilities, activities, and services to achieve an integrated joint network.

Cloud Computing

2-231. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources—networks, servers, storage, applications, and services—that can be rapidly provisioned and released with minimal management effort or service provider interaction. Users can access cloud services without geographic limitations, as long as they have a connection to the DODIN.

2-232. Cloud services may reside at a DOD core data center or be leased from a commercial cloud service provider. Units and commands can lease virtual servers or services to fulfill temporary requirements without going through the lengthy acquisition cycle and terminate the lease when they no longer need the services. Cloud-based solutions reduce the Army's ownership, operation, and sustainment costs for information technology hardware and software. Army units acquire cloud services through the DOD core data center, or acquire commercial cloud services according to the guidelines in Memorandum, DOD CIO, 15 December 2014, subject: Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services.

Defense Information Systems Network

2-233. The DISN is the DOD enterprise network for data, video, and voice services. DISN services include SIPRNET, NIPRNET, Joint Worldwide Intelligence Communications System, video teleconferencing, Defense Switched Network, Defense Red Switched Network, Defense Research Engineering Network, and mission partner environment.

2-234. The three segments of the DISN are the sustaining base, long-haul transport, and deployed. The long-haul segment provides network transport between the sustaining base and deployed network elements.

Satellite Transport

2-235. Satellite transport includes all DOD data and voice satellite communications. Satellite communications is a key method of network transport. Satellite communications capabilities, such as Wideband Global Satellite Communications, extend the DODIN worldwide to users without copper or fiber optic cable connections. Army satellite communications systems operate over military and commercial communications satellites. The extended range of satellite communications allows Signal forces to quickly establish connectivity within or between theaters. Using satellite communications transport allows Army

forces to extend access to the DODIN-A into remote or austere operational environments where there is no existing DODIN infrastructure.

Global Backbone (Fixed Station)

2-236. Strategic backbone transport connects theaters outside the continental United States to the DODIN. The backbone network transport establishes the DOD communications infrastructure and provides semi-permanent access to DISN services in garrison and training environments worldwide.

Gateway Access (Expeditionary)

2-237. DOD Gateways at select fixed satellite communications facilities provide deployed forces pre-positioned access points for reachback to the strategic support area. Because satellite communications allows beyond line of sight communications at great distances, it can extend immediate access to full DISN services in remote, austere operational environments without infrastructure limitations. Tactical satellite communications systems support command and control on-the-move as well as operations from traditional command posts. Refer to ATP 6-02.54 for more information about satellite communications transport.

Unified Capabilities

2-238. Unified capabilities integrate voice, video, and data services across a secure Internet protocol network. The services are independent of technology, so they do not require stand-alone systems to deliver capabilities. Using unified capabilities provides joint interoperability and reduces redundant efforts among the Military Services.

2-239. The Defense Information Systems Agency's unified capabilities approved products list is the single, consolidated list of products certified for interoperability and cybersecurity compliance. The approved products list includes network infrastructure capabilities as well as voice, video, and data services.

Note. The current list of approved unified capabilities is available at the Approved Products List Integrated Tracking System Website.

PERSONALLY IDENTIFIABLE INFORMATION

2-240. Personally identifiable information is any information that can be used to distinguish or trace an individual's identity. This information can be in hard copy or electronic format, stored on personal computers, laptops, and personal electronic devices, or found within databases. Protected personally identifiable information includes—

- Name.
- Social Security number.
- Date and place of birth.
- Mother's maiden name.
- Biometric records.
- Education records.
- Records of financial transactions.
- Medical files.
- Criminal records.
- Employment history.

2-241. In the digital age, leaked personally identifiable information can cause a great deal of damage. Many individuals have fallen victim to identity theft from leaked information. Data breaches can also compromise operations security or allow enemies or adversaries to target individual Soldiers or their family members.

2-242. Many DODIN users require access to some personally identifiable information in the regular course of their duties. Handling this information carries a special commitment to protect individuals' private

information. All Army military, civilian, and contractor employees whose duties require collecting, using, or storing personally identifiable information are responsible to—

- Be able to recognize and safeguard personal information.
- Collect personal information only when authorized and needed to perform their duties.
- Collect only the information necessary.
- Tell the individual the reason for collecting their personal information, who may see it, and what happens if the individual does not provide the requested information.
- Keep the information accurate, relevant, timely, and complete.
- Protect the information with encrypted storage.
- Transmit the information only with encryption and digital signature.
- Keep personally identifiable information confidential and protect it from misuse, loss, or data breach.

JOINT INFORMATION ENVIRONMENT

2-243. The joint information environment is a secure environment to share information technology infrastructure, enterprise services, and a single security architecture across the DODIN. The joint information environment implements enforceable standards and specifications, and common tactics, techniques, and procedures among the Services.

2-244. Security and interoperability of networked computers are configuration-dependent. A single incorrect setting on a workstation, router, or switch may leave it vulnerable to a cyberspace attack or unable to connect with the DODIN. Security affects every aspect of military operations. Likewise, interoperability is vital to mission success. Connecting to the DODIN facilitates collaboration with joint mission partners.

2-245. Each Service, installation, and organization has traditionally maintained separate security infrastructure and processes. This creates too many opportunities for failure and hinders information sharing among joint mission partners. Standardized, centralized security allows administrators to apply patches and improvements faster and with greater certainty.

2-246. The joint information environment improves operational effectiveness, standardizes training and equipment requirements across combatant commands and geographic regions, enhances security, and allows Services and agencies to allocate and align their information technology resources to their mission requirements. The joint information environment—

- Consolidates data centers.
- Standardizes and converges services, such as identity and access management and e-mail.
- Reduces the cyberspace attack surface.
- Provides DODIN-wide situational awareness.

Global Enterprise Operations Center

2-247. The Global Enterprise Operations Center is the Defense Information Systems Agency's top-level DODIN operations facility. The global enterprise operations center has complete visibility of the DODIN and oversees global DODIN operations to support combatant commanders. The global enterprise operations center—

- Directs global DODIN operations and defensive cyberspace operations-internal defensive measures.
- Prioritizes global cyberspace missions.
- Acts as the global focal point for integrating unified action partners into mission partner environment.
- Maintains global, joint situational awareness.

Enterprise Operations Center

2-248. The Defense Information Systems Agency's regionally-aligned enterprise operations centers maintain visibility of their respective portions of the enterprise network. The enterprise operations center conducts regional cyberspace missions to support geographic combatant commander priorities and those global missions directed by the global enterprise operations center. The enterprise operations center—

- Directs DODIN operations and defensive cyberspace operations-internal defensive measures in its assigned theater.
- Acts as the regional focal point for integrating unified action partners into mission partner environment.
- Maintains regional, joint situational awareness.
- Performs cybersecurity and defensive cyberspace operations-internal defensive measures functions, as directed by the global enterprise operations center.

Local Infrastructure (Base, Post, Camp, Station, or Joint Base)

2-249. The Services continue to maintain their local infrastructure and their ability to support tactical units and Service-unique missions. In the local infrastructure—

- The host Service maintains infrastructure.
- The host Service provides hands-on labor.
- The host Service provides defensive cyberspace operations incident response.
- The local installation provides mission- or unit-specific support.
- The Services maintain support for their tactical units.

Regional Top Level Architecture (Joint Regional Security Stack)

2-250. Top level architectures are access points to the DODIN. Their firewalls, intrusion detection, and intrusion prevention sensors represent the border security between the DODIN and the public Internet. In the legacy DODIN architecture, the Services typically hosted a top level architecture at each installation. Joint information environment replaces over 1,000 installation-based top level architectures with regional top level architectures (joint regional security stacks).

2-251. The joint regional security stacks consolidate the regional security architecture. This reduces the cyberspace attack surface by limiting the number of direct interfaces with outside networks. It also reduces the size of the specialized cybersecurity workforce needed to secure the network perimeter.

Note. Refer to *Enabling the Joint Information Environment: Shaping the Enterprise for the Conflicts of Tomorrow* for more information about the joint information environment.

JOINT THEATER DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS AUTHORITIES

2-252. The highest-level joint DODIN operations authority in a theater is the Defense Information Systems Agency's enterprise operations center (see paragraph 2-248). The geographic combatant command and joint task forces also have joint DODIN operations facilities to control their respective portions of the theater network.

Joint Cyberspace Center

2-253. A joint cyberspace center is the operational element of the combatant command that plans and oversees DODIN operations, defensive cyberspace operations, and offensive cyberspace operations in the theater. In conjunction with the theater network operations control center, the joint cyberspace center provides comprehensive network situational awareness, so commanders can make informed decisions to align network assets and capabilities to mission priorities and defend the network. Refer to JP 3-12 for more information about the joint cyberspace center's defensive and offensive cyberspace operations roles.

Geographic Combatant Command J-6

2-254. The geographic combatant command J-6 establishes policy and guidance for all communications assets supporting the joint force commander and develops communications system architectures and plans to support the geographic combatant commander's mission. The J-6 also advises the geographic combatant commander of the network's ability to support operations.

Theater Network Operations Control Center

2-255. The theater network operations control center is the geographic combatant command-level DODIN operations center. The theater network operations control center controls all theater systems and networks operated by forces assigned to or supporting the geographic combatant commander through technical channels.

Joint Network Operations Control Center

2-256. The commander, joint task force controls joint force systems and networks through a joint network operations control center. The joint network operations control center directs operations and defense of the joint task force portion of the theater network. The joint network operations control center collects network status from supporting units in the joint operations area for consolidated network situational awareness. The joint network operations control center provides the network status information to the joint cyberspace center for the theater-wide situational awareness view.

DEPARTMENT OF DEFENSE INFORMATION NETWORK-ARMY

2-257. The Army's portion of the DODIN is the DODIN-A. Adhering to common joint standards ensures interoperability and cybersecurity compliance across the entire Army enterprise and the wider DODIN. The DODIN-A uses redundant transport systems to link sensors, warfighting and business applications, and services. The network provides access to timely, accurate information in any environment and enables mission partner collaboration.

2-258. The DODIN-A connects geographically dispersed fixed station and deployed expeditionary forces to the global network through long-haul network transport, and supports—

- **Installation campus area networks** for known, verified users. Campus networks connect installation-based users to DISN services through a network enterprise center.
- **Regional hub nodes** that provide network transport and DISN services to support the deployed and training environments. The regional hub node includes a satellite transport component that connects deployed forces to the DODIN-A, and a gateway that provides access to DISN services and the wider DODIN.
- **Upper tier tactical internet** to connect deployed users to a data center and DISN services, regardless of their location. The deployed enclave connects to the DODIN-A and DISN services through the regional hub node or tactical hub node.
- **Lower tier tactical internet** infrastructure to support tactical formations down to the team leader.

2-259. Commanders and their staffs leverage the DODIN-A as a warfighting platform and the foundation for all other Army warfighting functions and capabilities. Commanders exercise command authority over their portions of the network. Signal units and Soldiers install, operate, and maintain their respective portions of the DODIN-A so commanders and staffs can communicate with higher, subordinate, adjacent, and supporting elements for mission success. The DODIN-A enables leaders to exercise command and control, integrate warfighting functions, and synchronize their efforts. The DODIN-A also allows synchronization with higher, subordinate, and adjacent units using the common operational picture and commander's intent, without needing direct control from higher headquarters.

ARCHITECTURE

2-260. The architecture of the DODIN-A provides access to protected services at the point of need. The architecture converges communications, computing, and enterprise services into a single platform that supports and enables all other missions and functions.

2-261. The core competencies and essential capability of the Signal Corps enable the DODIN-A's seamless cloud environment:

- **Network transport and information services** provide, and extend access to, the network and its applications and services.
- **DODIN operations and the essential capability of COMSEC** operate and secure the network and provide access to cloud-based services.
- **Spectrum management operations** enable those DODIN-A systems that rely on wireless connectivity, without causing or suffering unacceptable frequency interference.

Defense-in-Depth

2-262. Information systems security and network security are critical, because a single compromised workstation or networking device places the entire network at risk. DODIN operations personnel secure the network and its services through defense-in-depth. *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). Defense-in-depth includes perimeter security, enclave security, host security, physical security, personnel security, and cybersecurity policies and standards. Layered security protects every level of the network, down to individual workstations and users. By enhancing protection and survivability, defense-in-depth helps achieve the fundamental principle of trusted systems.

2-263. DODIN operations planners devise and implement comprehensive network plans using a full range of security measures. The plan includes both external and internal perimeter protection. External perimeter protection consists of COMSEC procedures, router filtering, access control lists, security guards, and, where necessary, physical isolation serving as a barrier to outside networks, such as the public Internet. Internal perimeter protection consists of firewalls and router filtering. These serve as barriers between echelons of interconnected networks and information systems. Internal COMSEC barriers provide another layer of security for network enclaves. Local workstation protection consists of individual access controls, configuration audit capability, protection and intrusion detection tools, and security procedures.

2-264. The joint regional security stack secures the logical boundary between the DODIN-A and the rest of the DODIN. The hardened outer perimeter of the joint regional security stack controls access to applications and data within the DODIN-A.

Communications in Depth

2-265. Network-enabled operations require a robust, survivable network. Maintaining network-enabled capabilities in a degraded information environment mandates a communications in depth architecture for the tactical portion of the network. Deployed signal elements implement redundant network transport using line of sight transport, satellite communications, wire, and cable. Automatic network establishment and restoral eliminate single points of failure so critical communications still get through. Refer to ATP 6-02.60 for more information about tactical network systems.

Colorless Core

2-266. Colorless core is a Defense Information Systems Agency-compliant cybersecurity architecture that offers more efficient Internet protocol network encryption and transport. The key benefits of colorless core are data protection and more efficient bandwidth use. The colorless core architecture encrypts all data, whether classified or unclassified, from end-to-end. This is different from legacy systems that only encrypted classified information. Since all the encrypted data looks the same, an enemy or adversary cannot distinguish between classified and unclassified data. 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.

Link layer encryption isolates the network backbone (the wide-area network) from external networks. Refer to ATP 6-02.60 for more information about colorless core architecture.

Transport Convergence

2-267. The Army has long maintained separate tactical transport networks to support the communications requirements of different functional areas—command and control, intelligence, logistics, and medical. A unit with all of these networks has used four separate satellite communications terminals and four sets of networking hardware with all the associated manning, physical security, configuration and patching, and logistics support requirements; four separate DODIN operations chains of authority; and up to four separate commercial satellite leases. Converging the transport for these networks onto a common network transport medium makes better use of resources and assets, leverages existing infrastructure, increases network security, and simplifies network management, while reducing reliance on leased commercial satellite resources.

2-268. The Army is migrating the network transport for the tactical portions of these networks onto a single transport medium using the colorless core architecture. The first phase of transport convergence integrates the top secret/sensitive compartmented information intelligence network into the colorless core architecture to brigade level in the deployed portion of the network. The sensitive compartmented information data is encrypted end-to-end from the TROJAN Network Control Center to the G-2 (S-2) section. The signal systems provide only network transport. The G-2 (S-2) section continues to perform DODIN operations functions for top secret networks.

2-269. The extra demand for data throughput over the converged transport requires DODIN operations personnel to manage bandwidth apportionment and quality of service rules for the different classes of data, based on mission requirements. Bandwidth apportionment ensures the converged transport provides the same quality services as the legacy capabilities.

OPERATING ENVIRONMENTS

2-270. Work, deployed, and home or mobile represent the DODIN-A operating environments. Sharing configurations and security standards allows these environments to operate as a single, integrated network.

Work Environment

2-271. Generating forces occupy posts, camps, and stations worldwide supporting the geographic combatant commanders. The work environment represents the Army in-garrison, using the DODIN-A as a strategic capability to support the generating force and shaping operations. Forward-deployed posts, camps, and stations rely on Defense Information Systems Agency long-haul transport for connection to enterprise services.

Network Enterprise Center

2-272. The *network enterprise center* is the facility that provides and acquires telecommunications and information management services on Army installations (ATP 6-02.71). The network enterprise center manages the installation campus area network and ensures service quality for supported units at their home station. The campus area network connects installation-based users to the DISN, secure data stores, and baseline common services on a non-reimbursable basis. The network enterprise center provides information technology services other than those on the baseline services list on a fee-for-service basis (refer to AR 25-1). Strategic signal battalions operate the network enterprise centers. The network enterprise center delivers these baseline services to units in garrison:

- Communications systems and system support services.
- Telephone and data infrastructure services.
- Emergency communications telephone services.
- Wireless infrastructure services.
- Video teleconferencing services.
- Range and field telephone services.

- Telecommunications continuity of operations plan and operation plan support services.
- Fire, safety, security, and other circuit services.
- Non-tactical radios and non-tactical/tactical radio spectrum management services.
- Cybersecurity services.
- Defense-in-depth.
- COMSEC services.
- Risk management, accreditation, and certification policy services.
- Network security services.
- Automation services.
- Mail, messaging, and collaboration (Defense Enterprise E-mail and Organizational Messaging Service) and storage services.
- Desktop, software, and peripheral support services.
- Web support services.
- Automation and network service support services.

Note. Refer to the Command, Control, Communications, Computers, and Information Management Services List for information about baseline common services.

Installation as a Docking Station

2-273. Securing tactical networks is complex and requires Soldiers proficient in specialized technical skills. These skills are perishable and degrade quickly if not exercised regularly. Installation as a docking station provides a standardized, simplified connection between mission command information systems and the installation network. This allows units to train and work with the same systems they use when deployed without relying on costly commercial satellite bandwidth or limited military satellite bandwidth and regional hub node availability. Units can use the same systems and software they use on the battlefield as a routine element of daily operations at their home station.

2-274. Installation as a docking station reduces the time needed to establish cybersecurity-compliant tactical networking components through an always-on concept. The local network enterprise center distributes patches directly to the unit, so system administrators can apply them immediately. This keeps user accounts current and systems patched to mitigate security vulnerabilities. Because the system patching stays up to date, the systems can rapidly transition to and from an operational theater. Units only need to pack their equipment and begin movement.

2-275. Commanders and staffs can access the forward-deployed network and mission partner environment through installation as a docking station. Theater and mission-specific information stores are available at the home station to support the operations process. Installation as a docking station enables planning, preparing, and assessing operations on the same mission network used in the operational theater.

Home Station Mission Command

2-276. Advances in communications and information technologies, such as teleconferencing and other remote collaboration capabilities, allow units to conduct split-based operations, where the tactical command post deploys to an operational theater and the main command post continues to operate from home station. Each Army division has a home station mission command center that allows its main command post to control operations of deployed, deploying, and non-deployed subordinate units from its home station. A tailored portion of the headquarters can deploy to an area of operations and establish either an early entry command post or a forward-deployed command post. The remainder of the headquarters can operate from home station to perform dedicated analysis, planning, and coordination supporting forward operations.

2-277. Home station mission command reduces the time and strategic lift resources required to deploy a division command post. It also reduces the forward logistics footprint required to sustain the command post as compared with supporting an entire division headquarters.

2-278. The size of the early entry or forward-deployed command post can increase or decrease as necessary in response to changes in the operational or mission variables. Large-scale combat operations and campaigns or unacceptable network defense challenges may require the division headquarters to deploy most of its command and control capabilities. In these cases, the entire headquarters can deploy and establish traditional main and tactical command posts in the operational theater.

2-279. Home station mission command increases data throughput requirements between deployed elements and the home station headquarters. Signal planners should consider the network architecture and data requirements for reliable connectivity between the separate headquarters. Locally hosting services at each end so users can access critical information without relying on reachback mitigates the data throughput requirements.

Deployed Environment

2-280. The strategic infrastructure supports units' requirements at their home station, but tactical units still need communications and information services when deployed in an operational theater. The deployed portion of the DODIN-A provides the needed services and supports tactical mobility requirements.

2-281. The regional cyber center manages the theater network through technical channels. Deployed tactical forces connect to the DODIN-A using satellite transport through a DOD Gateway site, regional hub node, or tactical hub node. The tactical portion of the DODIN-A extends DISN voice, data, imagery, and video capabilities to deployed forces.

Home or Mobile Environment

2-282. Many authorized users operate from outside the boundaries of the Army network. These users access the DODIN-A from home or a temporary duty location. These users usually connect with the network through the public Internet or a virtual private network connection. Users within the home and mobile environments access the DODIN through commercial telecommunications to a joint, Army, or other Service network entry point.

2-283. The security of an enterprise network is only as strong as its weakest point. Secure data, applications, and services depend on cybersecurity compliance. Users must maintain current antivirus software and follow good security practices. The DODIN-A operational view (Figure 2-3 on page 2-51) shows a high-level overview of the DODIN and DODIN-A.

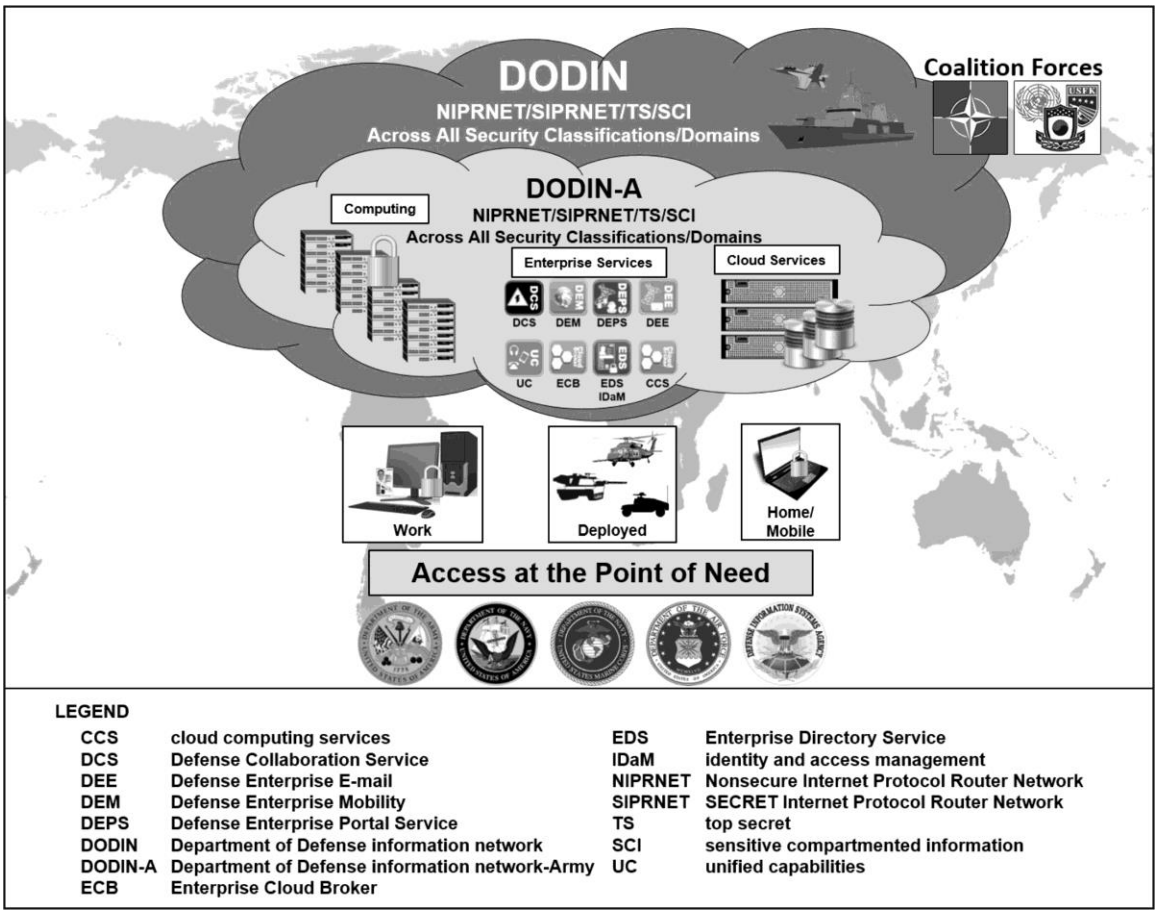


Figure 2-3. Department of Defense information network-Army operational view

This page intentionally left blank.

Chapter 3

Signal Support to Operations to Shape and Prevent

This chapter provides an overview of signal support to Army operations to shape and prevent. Section I discusses signal support in Army operations to shape. Section II discusses signal support in Army operations to prevent.

SECTION I – OPERATIONS TO SHAPE

3-1. Operations to shape consist of various long-term military engagements, security cooperation, and deterrence missions, tasks, and actions intended to assure friends, build partner capacity and capability, and promote regional stability (FM 3-0).

OVERVIEW OF ARMY OPERATIONS TO SHAPE

3-2. Operations to shape support the geographic combatant commander's theater campaign plan or the theater security cooperation plan. Operations to shape serve four primary purposes:

- Promoting and protecting U.S. national interests and influence.
- Building partner capacity and partnerships.
- Recognizing and countering adversary attempts to gain positions of relative advantage.
- Setting conditions to win future conflicts.

3-3. Shaping activities include unit home station activities such as maintaining operational readiness, training, contingency planning, combined exercises and training, military exchange programs, security cooperation, and military-to-military engagements. Figure 3-1 on page 3-2 depicts activities to shape operational environments and prevent conflict in an environment of cooperation and competition. Army forces conduct shaping activities as part of a joint team and a larger whole-of-government effort to assure friends, build partners, and to prevent, deter, or turn back adversary escalation.

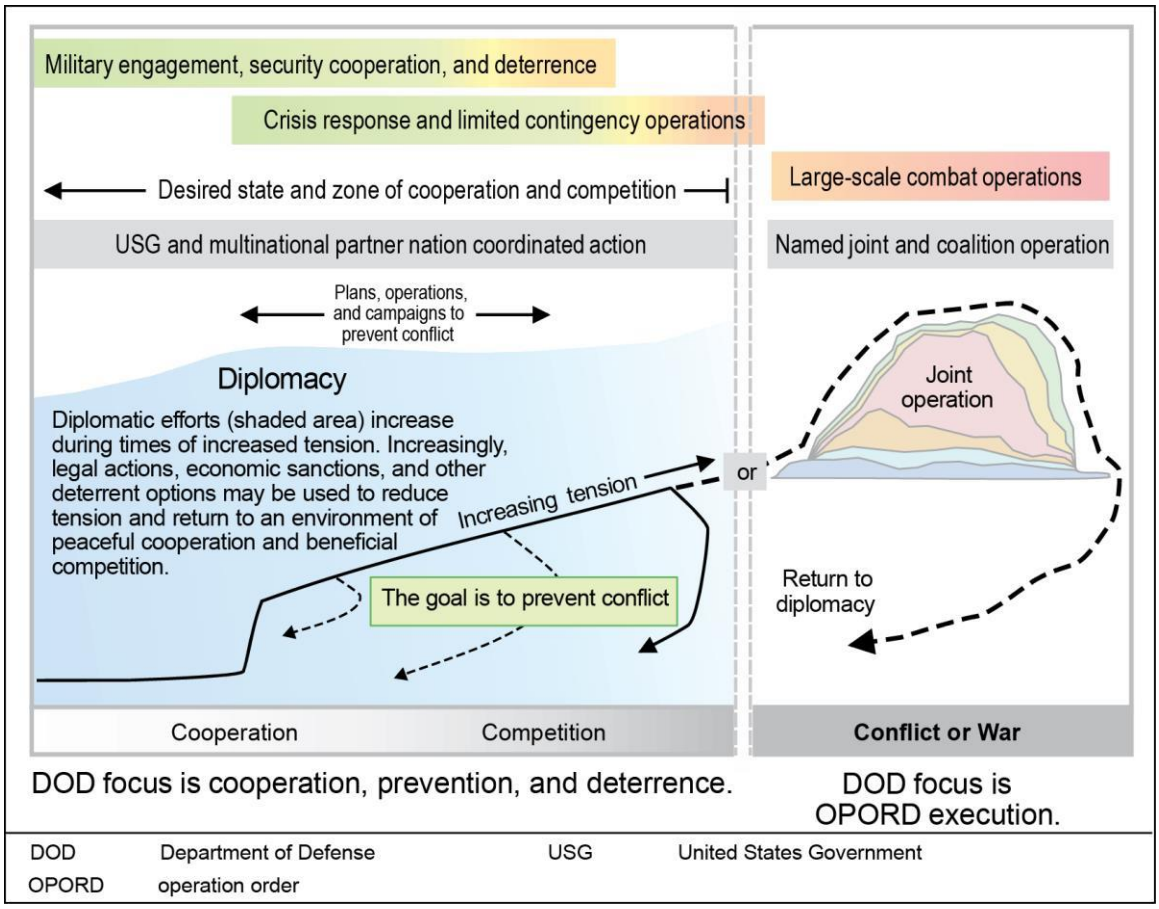


Figure 3-1. Shaping activities within an environment of cooperation and competition

3-4. Shaping activities help assure operational access for crisis response and contingency operations. Army signal forces support the geographic combatant commander's shaping operations to promote favorable access. Signal activities that support shaping operations include—

- Key leader engagements.
- Bilateral and multinational exercises to improve multinational communications interoperability.
- Negotiations to develop bilateral and multinational information sharing agreements.
- The use of grants and contracts to improve interoperability and the communications capabilities of partner nations.
- Designing interoperability into acquisition programs.
- Agreements for shared use of the electromagnetic spectrum.
- Mapping of adversary capabilities in the electromagnetic spectrum.

Signal Support to Security Force Assistance and Long-Term Consolidation of Gains—Colombia

U.S. communications capabilities supported the government of Colombia as it confronted the destabilizing challenges of the Revolutionary Armed Forces of Colombia. Through various long-term programs, the United States aided Colombian forces in their struggle against a protracted, bloody insurgency that at times controlled significant areas of the country.

One of the programs was the development of bilateral information sharing agreements and the provisioning of a coalition network. The coalition network was a secure, secret-releasable communications network that linked more than 25 key Colombian command and control nodes, support elements from the United States Southern Command, and other U.S. Government agencies.

The coalition network enabled the Army to provide technical, planning, and operational assistance to Colombian National Police and military forces, and fully integrate the military approach into interagency efforts. Improved, secure information sharing during police and military operations strengthened capabilities. The ability to share information reduced operational friction between friendly forces, increased the effectiveness of Colombian security forces, and bolstered their capacity.

These capacity-building activities weakened transnational drug cartels and the Revolutionary Armed Forces of Colombia, while fostering a culture of cooperation and information sharing in rising generations of Colombian military and government personnel. Ultimately, that made them more effective in current and future operations.

SIGNAL OPERATIONS ASSESSMENTS

3-5. Signal operations assessments are integral to planning and executing communications support. Operations assessments identify and analyze changes in the operational environment and determine the success of signal elements supporting the campaign or operation. Signal operations assessments help the theater army G-6 develop, adapt, and refine the theater communications support plan.

3-6. Collecting information to develop an understanding of the operational variables provides the basis for signal operations assessments. A complete understanding of the operational environment, the theater campaign plan, and the commander's priorities is critical to developing an accurate assessment.

RISKS TO SIGNAL SUPPORT

3-7. Enemies and adversaries will attempt to further their interests and achieve their goals without fighting. Threat actors will focus on disrupting and degrading networks and intercepting or manipulating information to undermine unified action partner relationships, raise political stakes, shape public opinion, and challenge U.S. resolve. The goal of threat activities during shaping operations is limiting allied action and freedom of maneuver.

3-8. Cyberspace attacks may allow an enemy or adversary to extract sensitive information, contingency plans, or other data to degrade relationships or mitigate planned friendly operations. Adversaries may conduct reconnaissance in cyberspace to identify vulnerabilities in friendly networks, so they can plan cyberspace attacks to disrupt friendly forces' ability to respond during crisis. Signal forces maintain cybersecurity compliance to prevent intrusions into the DODIN-A.

SIGNAL SUPPORT

3-9. Shaping activities take place continuously within a theater. The geographic combatant commander uses shaping activities to improve partner nations' internal security, enhance international legitimacy, gain multinational cooperation, and influence adversary decision making. Shaping activities tie directly to authorities provided in the United States Code and approved programs. The geographic combatant commander integrates and synchronizes shaping activities with the Department of State, other government agencies, country teams, and ambassadors' plans and objectives. Mission partners develop and synchronize shaping activities in the country plan, the geographic combatant commander's theater strategy, and the theater campaign plan.

3-10. Signal forces supporting shaping operations provide communications capabilities to the geographic combatant commander and Army forces in theater. Signal support to shaping operations may also include signal-focused security cooperation activities with partner agencies and countries.

MILITARY ENGAGEMENT

3-11. *Military engagement* is the routine contact and interaction between individuals or elements of the United States Armed Forces and those of another nation's armed forces or civilian authorities to build trust and confidence, share information, coordinate mutual activities, and maintain influence (JP 3-0). Geographic combatant commanders seek out partners and communicate with adversaries to discover areas of common interest and tension. Such military engagements can reduce tensions and may prevent conflict or build coalitions.

3-12. The theater army G-6 provides communications capabilities to support military engagements by allocating mobile communications capabilities or providing information technology support to key leader engagements. The G-6 may also conduct key leader engagements with partner nations to establish relationships and develop plans for further assistance or cooperation.

SECURITY COOPERATION

3-13. Commanders and staffs conduct security cooperation to develop allied and friendly military capabilities for self-defense and multinational operations. Security cooperation activities improve information exchange and intelligence sharing, provide U.S. forces with peacetime and contingency access, and mitigate conditions that could lead to crisis. Commanders execute various security cooperation activities such as the transfer of defense articles and services to eligible foreign governments, training and education of foreign military personnel, the sale of construction services to develop a host nation's internal defense, and developing programs to build partner capabilities and capacity for self-sufficiency. Security cooperation activities include:

- Security assistance.
- Security force assistance.
- Foreign internal defense.
- Security reform.

3-14. Although each security cooperation activity is unique, signal support for each activity is similar. The signal support plan depends on the desired outcome of the theater campaign plan.

3-15. Signal subject matter expert exchanges, training, and education are investments in the future of the host nation's military institutions. These security cooperation activities foster future cooperation and build partner-nation capacity. Sharing information on tactics, techniques and procedures, interoperability, and doctrine provides a path to self-sufficiency and builds relationships between U.S. and partner nation militaries. Multinational signal-themed symposiums enable sharing of information and ideas between foreign countries and often result in better tailored, peer-nation solutions. Refer to FM 3-22 for a more detailed discussion of Army support to security cooperation.

INTEROPERABILITY

3-16. Single-channel very high frequency (VHF), high frequency (HF), and tactical satellite radios provided through grants, loans, or foreign military sales build partner-nation military communications capabilities, capacity, and command and control interoperability. Secure radios for loan or sale to partner nations are unique for foreign release, but are interoperable with, and share most of the same features of, those used by U.S. forces. Country teams maintain accountability of loaned radios and facilitate the transfer of COMSEC keying material for the systems. Some radios, such as single-channel ground and airborne radio system, are not approved for foreign release and cannot be loaned to foreign governments or militaries. When the United States provides radios as part of a grant, loan, or sale, planning for ongoing logistics support is critical to maintaining the operational capability of the system.

3-17. Working closely with allies and partners is a key and enduring element of U.S. national strategy. The United States frequently needs support from its partners and allies to prevail in contemporary conflicts. Likewise, U.S. partners and allies often need extensive U.S. support during regional and internal conflicts (ATP 3-94.1). Establishing among military headquarters allows commanders to integrate with joint, inter-organizational, and multinational mission partners by providing staff interface, mentoring, support, and communication required for U.S. partners to accomplish their missions.

MULTINATIONAL NETWORKS

3-18. The development of regional or theater classified information sharing arrangements and command and control networks fosters cooperation between the United States and partner nations. U.S. forces and allies employ both sustained and ad hoc bilateral and multinational networks to practice command and control of multinational operations during exercises, and support to day-to-day operations across the Army's strategic roles of shape, prevent, conduct large-scale ground combat, and consolidate gains.

3-19. As the DOD executive agent for theater communications infrastructure, the Army is often the lead for installing, operating, maintaining, and securing bilateral and multinational information sharing networks. Coalition networks connect partner nation-owned networks to the core of the DODIN. If partners do not have the capacity, the geographic combatant commander may loan the necessary equipment.

3-20. The Defense Information Systems Agency establishes technical and operational standards for mission partner environment. Sharing common configurations and operating procedures among multinational mission partners removes the barriers to information sharing.

3-21. Although there are U.S. encryption devices available for release to foreign nations, some constraints apply to which countries may possess, control, and operate the equipment. Providing COMSEC materials and equipment to a foreign nation requires a formal COMSEC sharing agreement and a bilateral command and control interoperability board. The command and control interoperability board guides the partner nation through the process of establishing a U.S. COMSEC account with adequate secure storage facilities, and provides a venue to develop further interoperability programs. The National Security Agency-approved commercial solution for classified may serve as an alternative to U.S. COMSEC equipment and materials. The commercial solution for classified is an end-to-end commercial encryption solution that is releasable to friendly foreign nations and approved to transmit sensitive information.

CYBERSECURITY

3-22. The security of a multinational network is only as strong as the partner nations operating on it. Most partner nations are in the early development of cybersecurity programs. Army cybersecurity professionals can share lessons learned with partner nations as they develop their programs. Sharing cybersecurity tactics, techniques, procedures, and insights from U.S. Army experience can help partner nations establish or improve their cybersecurity programs and capabilities.

3-23. All nations must share a common system baseline and conduct disciplined cybersecurity programs to prevent unnecessary vulnerabilities to the network and the data it carries. Cybersecurity processes to preserve information and information systems include—

- The risk management framework.
- Integration and interoperability.

- Protecting DOD information.
- Identity and access management.

3-24. Sharing cybersecurity program information and threat warnings builds trust and confidence between the Army and unified action partners. Timely and deliberate information sharing maximizes the security of critical network infrastructure. Cybersecurity and network defense personnel must share vulnerability information to the maximum extent allowed by law, regulation, and government-wide policy. The geographic combatant command J-6 and theater army G-6 develop guidance and programs for sharing cybersecurity information. The theater army is the cybersecurity lead for any coalition network provided by the Army.

SUPPORT TO DEFENSIVE AND OFFENSIVE CYBERSPACE OPERATIONS

3-25. The DODIN-A faces continuous risk from threat actors. Signal planners collaborate with the CEMA section to help identify key terrain in cyberspace during operations to shape. The CEMA section plans for defensive cyberspace operations support. Cyberspace capabilities must be coordinated, built, moved, and provided access to various nodes across cyberspace. These systems require constant maintenance and defense throughout operations to shape.

3-26. Defensive cyberspace operations require access to the theater network. DODIN operations personnel collaborate with defensive and offensive cyberspace operations personnel throughout the planning process, since their activities are interdependent.

ADDITIONAL SHAPING ACTIVITIES

3-27. As part of operations to shape, Army signal forces conduct numerous other activities supporting the geographic combatant command and theater army. These include signal support to intelligence operations, support to countering weapons of mass destruction, support to humanitarian efforts, and organizing and participating in combined training and exercises.

SUPPORT TO INTELLIGENCE OPERATIONS DURING SHAPING ACTIVITIES

3-28. The theater military intelligence brigade-theater provides regionally-focused collection and analysis to support the geographic combatant commander, theater army commander, and Army forces conducting operations to shape. The theater military intelligence brigade has S-6 staff support and dedicated satellite transport systems for sensitive compartmented information networks. With transport convergence (see paragraph 2-267), tactical signal systems replace the dedicated intelligence transport systems for sensitive compartmented information networks.

3-29. Units at home station access sensitive compartmented information networks, SIPRNET, NIPRNET, and coalition networks through the DODIN-A fixed infrastructure. In a deployed environment, Warfighter Information Network-Tactical provides satellite transport for top secret/sensitive compartmented information networks to the brigade level. If the military intelligence brigade identifies network requirements beyond the capability or capacity of organic signal assets, they request additional signal support through the theater army and geographic combatant command. Signal support comes from theater-available assets or elements of an expeditionary signal battalion. See appendix E for more information about requests for signal support.

SUPPORT TO COUNTERING WEAPONS OF MASS DESTRUCTION

3-30. Shaping activities work toward strategic deterrence of weapons of mass destruction. Army forces shape an operational environment to dissuade or deter adversaries from developing, acquiring, proliferating, or using weapons of mass destruction.

3-31. The DODIN-A fixed infrastructure supports the countering weapons of mass destruction mission. Units conducting countering weapons of mass destruction missions use their organic signal capabilities. When organic capabilities cannot meet mission requirements, these units request additional support through the theater army and geographic combatant command.

SUPPORT TO HUMANITARIAN EFFORTS

3-32. The United States Agency for International Development collaborates with Army forces for humanitarian relief missions. Security cooperation efforts include exercises in preparation for theater humanitarian missions.

3-33. Communications support ranges widely from secure and nonsecure cellular phones to wideband, deployable network nodes. Signal support to humanitarian relief depends on the size and scope of the operation. Signal elements supporting humanitarian efforts may need to directly support U.S. Government interagency partners, non-governmental organizations, host-nation government agencies, and media outlets when no other communications capabilities exist.

Humanitarian Assistance: Hurricane Matthew, U.S. Military Support to Haiti

On October 4, 2016, Haiti was hit by 140 mile per hour winds from category 4 Hurricane Matthew, leaving a swath of destroyed homes, stripped trees, raging rivers, and flooded streets. The storm dumped over two feet of rainwater on the island within 24 hours.

Commander, United States Southern Command, along with numerous governmental and non-governmental agencies, was poised to provide emergency humanitarian support.

Within hours of the storm's passing, the Joint Task Force (JTF) Matthew commander arrived to assess damage and develop the plan for emergency assistance. The initial joint task force communications capability consisted of nonsecure cellular telephones, secure satellite telephone service, and single-channel tactical satellite. The first commander's update brief to the United States Southern Command staff took place by conference call over the secure satellite phone.

Concurrently with the JTF-Matthew commander's assessment, Army and Marine Corps helicopters self-deployed from JTF-Bravo in Honduras. As the helicopters deployed, the JTF-Bravo commander maintained en route communications with the JTF-Matthew commander and the United States Southern Command staff using single-channel tactical satellite and secure satellite telephones.

As the end-strength of JTF-Matthew grew to roughly 400 Soldiers and sailors, the 1st Joint Communications Squadron of the Joint Communications Support Element deployed a satellite communications terminal to support the JTF headquarters with secure video teleconferencing, telephone, chat, and data services. In the end, the mission lasted 14 days and distributed 253 metric tons of relief supplies to areas of the country unreachable by land routes.

SUPPORT TO COMBINED TRAINING AND EXERCISES

3-34. Combined training and multinational exercises play a key role in shaping an operational environment and setting the conditions for the geographic combatant commander to initiate rapid crisis action. Signal support to combined training and exercises varies from information technology support, to exercise simulations, to fully-deployed communications networks supporting large troop formations.

3-35. It is important to exercise the full communications capabilities anticipated for use in a crisis. Training events that use the full network validate tactics, techniques, and procedures, battle drills, and policies for employing and operating the network. Realistic exercises help identify what services are required to support

the geographic combatant command and theater army. Using mission partner environment during combined exercises ensures multinational mission partners can share information with these systems during operations.

CONSOLIDATING GAINS

3-36. Security cooperation helps set the theater for future geographic combatant command and theater army actions. Security cooperation activities address interoperability, validate standard operating procedures, and exercise communications systems to prepare the multinational force to rapidly respond to crises or transition to operations to prevent. Signal forces and staffs consolidate gains in signal support during operations to shape by adjusting the scheme of signal support in operation plans to address changing communications requirements.

SECTION II – OPERATIONS TO PREVENT

3-37. The purpose of operations to prevent is to deter adversary actions contrary to U.S. interests. They are typically conducted in response to activities that threaten unified action partners and require the deployment or repositioning of credible forces in a theater to demonstrate the willingness to fight if deterrence fails (FM 3-0).

OVERVIEW OF ARMY OPERATIONS TO PREVENT

3-38. Prevent activities enable the joint force to gain positions of relative advantage prior to future combat operations. Operations to prevent are characterized by actions to protect friendly forces and indicate the intent to execute subsequent phases of a planned operation (FM 3-0). Army forces perform the following major activities during operations to prevent:

- Execute flexible deterrent options and flexible response options.
- Set the theater.
- Tailor Army forces.
- Project the force.

3-39. Signal support in operations to prevent requires signal leaders and organizations to quickly plan support, engineer network solutions, and deploy personnel and equipment in support of expeditionary Army forces. Signal planners and units tailor communications packages to minimize the communications footprint while providing robust communications capabilities to the deploying force. Signal capabilities support en route services, echeloned command posts, and ad hoc requirements.

3-40. During operations to prevent, the theater army G-6, the SC(T) commander, and theater tactical signal brigade commander contribute to joint command and control by establishing, maintaining, and securing the network architecture to support joint and Army forces operating in theater.

3-41. The theater portion of the DODIN-A provides network and information system availability, information protection, and information delivery across the strategic, operational, and tactical levels. Signal units provide the theater army with trained and ready signal Soldiers to support Army operations to prevent and rapidly transition to combat operations, if required.

RISKS TO SIGNAL SUPPORT

3-42. During operations to prevent, peer threats shift resources to information warfare and preclusion. Threat supporting efforts include systems warfare and sanctuary. Threat forces will consider four key areas when designing operations to mitigate U.S. deterrence efforts. They include—

- Attempts to reduce the perceived risk to threat forces.
- Limited attacks to expose friendly vulnerabilities.
- Deception operations to conceal the threat's true intentions.
- Attempts to slow and disrupt deployment to limit U.S. force buildup.

3-43. Peer threats can focus these methods against U.S. forces' ability to establish communications networks and critical command and control nodes. Preventing effective communications between command and control nodes through limited cyberspace or electronic attacks will disrupt synchronization of operations and logistic support, disrupt deployment, and damage credibility among multinational mission partners.

SIGNAL SUPPORT

3-44. In support of Army activities to prevent, signal units execute technical response options and establish communications capabilities at key command and control and logistics nodes. Technical response options defend critical communications networks and nodes. Technical response options include establishing backup circuits for key nodes, strengthening cybersecurity measures, and shifting network resources for emergency circuit restoral. Planners tailor communications packages to mission requirements and prepare or execute communications support plans for deploying Army forces.

3-45. As the Army executes flexible deterrent options and flexible response options, supporting signal elements employ strategic and expeditionary communications capabilities to meet emerging requirements. The joint force J-6 and Army component G-6 coordinate to shift resources, activate pre-planned circuit requirements, reengineer satellite capabilities, allocate electromagnetic spectrum access, and prepare to provide contract resources to support the force.

3-46. The theater army plans and coordinates Army capabilities to meet the geographic combatant commander's intent to set the theater. Given the expected time to deploy additional capabilities, the theater army G-6 coordinates with the commander and staff to identify strategic and tactical signal capabilities for forward-deployment to support immediate communications requirements as deploying units arrive in the theater. Support requirements include—

- Joint command and control requirements.
- Port and terminal operations.
- Intermediate staging base support.
- Reception, staging, onward movement, and integration support.
- Noncombatant evacuation operation requirements.
- Emergency circuit restoral.
- Logistics node support.

TAILORING SIGNAL CAPABILITIES

3-47. Tailoring signal capabilities is selecting the right capability and deploying in the optimal sequence. The theater army G-6 staff maintains operational focus in determining signal support requirements. Tailored capabilities match the size, capacity, flexibility, and capability of signal force packages to support the requirements of the operation plan.

SIGNAL SUPPORT TO FORCE PROJECTION

3-48. *Force projection* is the ability to project the military instrument of national power from the United States or another theater, in response to requirements for military operations (JP 3-0). Speed and combat readiness are essential to achieving the desired position of advantage over an adversary.

SIGNAL DEPLOYMENT

3-49. Understanding the geographic combatant commander's intent and operation plan is the foundation of signal deployment planning. Signal deployment plans establish what capabilities are needed, by location and time, for successful deployment outcomes. The theater army G-6 should consider—

- Geographic combatant command and theater army operation plans.
- Geography and the effects of terrain and distance on terrestrial-based communications.
- Threat capabilities to disrupt, degrade, or destroy communications capabilities.
- Tactical dispersion of signal capabilities.

- Separation of signal sites from the supported command post (remoting) to reduce command post vulnerabilities.
- Available signal capabilities—type, size, and numbers:
  - Strategic.
  - Host-nation.
  - Multinational partners.
- PACE plan.
- Capability gaps by requirement and system.
- Size and location of command and control nodes, including the number of network users at each node.
- Other key headquarters requiring communications support—size and locations.
- Data threads—understanding what systems or command posts must communicate where.
- Satellite, electromagnetic spectrum, and communications capacity and availability to support the operation, including single-channel availability.
- Services required—data, voice, and video, by location.
- Quality of service—prioritization of key leaders, command posts, and types of data on the network.
- Protection of critical nodes—the communications capabilities most critical to the success of the joint force and the Army component, and plans to protect those capabilities and nodes.
- DODIN operations—define responsibilities for managing and controlling portions of the network and determine availability of DODIN operations tools.
- Cybersecurity—the theater cybersecurity program and management plan.
- Coordination for defensive and offensive cyberspace operations support—
  - Organization, planning, and execution.
  - Support requirements.
- Transition plan to shift from tactical signal to fixed infrastructure, including resources available or needed.
- Capabilities available for the commander at key locations and times throughout the operation.
- Authorizing official who approves devices and software on the network.
- Mission command information systems—
  - Locations.
  - Paths to servers.
  - Software versions.
  - Configurations.
  - Effects of network latency.
- Maintenance management and tracking.
- Key battle rhythm events—
  - Systems used.
  - Times.
  - Locations.
  - Requirements.
- COMSEC requirements—plan for distribution, accounting, and security of cryptographic keying material.

NETWORK AND DATA PROTECTION WHILE THE FORCE IS IN TRANSIT

3-50. As the Army force is in transit, the risk to operations increases. Units operate with limited communications capabilities and redundancy, and have minimal defensive capabilities while en route to an operational area. The peer threat will use this to their advantage. Threat actors may conduct cyberspace or electronic attacks to disrupt the flow of information in an attempt to impede or prevent unit deployments.

Disrupting the ability of Army forces to track the identity, status, and location of units, personnel, and cargo may cause delays in deployment, desynchronize force deployment plans, and disrupt U.S. forces' ability to quickly build combat power.

3-51. The theater army G-6 coordinates technical response options to implement cybersecurity in the theater portion of the DODIN-A. Enforcing encryption standards, minimizing non-essential use of the commercial Internet, validating connected devices, and enforcing strict network authentication are some of the technical response options the G-6 can implement to improve the network's cybersecurity posture. The joint force J-6 coordinates with the operations directorate of a joint staff (J-3) and the joint cyberspace center to deploy cyberspace defense forces and to conduct threat-based analysis, monitoring, and vulnerability mitigation on key terrain in cyberspace.

RECEPTION, STAGING, ONWARD MOVEMENT, AND INTEGRATION

3-52. Reception, staging, onward movement, and integration delivers combat power to the joint force commander in a theater of operations or a joint operations area (FM 3-0). Signal elements supporting reception, staging, onward movement, and integration provide the theater army and arriving units the communications capabilities necessary to enable command and control and track personnel and equipment as they transit ports of debarkation and staging areas to enable rapid onward movement.

3-53. During reception and staging, signal units provide fixed infrastructure or tactical signal support at ports of debarkation and staging bases to enable the unit's reception, staging, onward movement, and integration. Tactical communications systems not configured to operate in the theater before deployment do so during staging. Deploying units test and validate their radios and network systems, as time permits.

3-54. Theater army, corps, and division G-6s plan signal support for emergency road and route communications, casualty evacuation, route control, and other specialized communications requirements during onward movement. Units should limit nonsecure cellphone use because of the vulnerability it brings to operations. The theater tactical signal brigade deploys to exercise command and control of expeditionary signal battalions and augments the corps network operations and security center or joint network operations control center to provide DODIN operations oversight for tactical networks.

3-55. During integration, signal elements continue to support unit arrivals, begin integrating their network systems into the theater network, and establish network situational awareness so they can monitor and track the installation, operation, maintenance, and security of the network. The theater tactical signal brigade works directly with the Army component G-6 or the joint force J-6 as the central focal point for all network activities.

CONSOLIDATING GAINS

3-56. The primary signal tasks in consolidating gains during operations to prevent are planning efforts to migrate to fixed infrastructure when and where possible and planning support for follow-on forces specifically tasked to consolidate gains. Thorough signal planning and preparation for support to offensive, defensive, and stability tasks enable positive future security and stability outcomes.

3-57. Signal commanders and staffs plan for the eventual expansion of consolidation areas, as well as supporting the command structure responsible for those areas as large-scale combat operations continue. Tactical signal capabilities support communications requirements while fixed communications infrastructure is being built out in consolidation areas. Planning for rapid network expansion is a critical part of signal support in operations to prevent.

This page intentionally left blank.

Chapter 4
Large-Scale Combat Operations

This chapter discusses signal support to large-scale combat operations. The chapter is divided into 4 sections. Section I provides an overview of signal support to joint and Army large-scale combat operations. Section II discusses signal support in large-scale defense operations. Section III discusses signal support in large-scale offensive operations. Section IV discusses signal support to the consolidation of gains in large-scale combat operations.

SECTION I – SIGNAL SUPPORT TO LARGE-SCALE COMBAT OPERATIONS

OVERVIEW OF LARGE-SCALE COMBAT OPERATIONS

4-1. The nature and scope of some missions may require joint forces to conduct large-scale combat operations to achieve national strategic objectives or protect national interests. Such combat typically occurs within the framework of a major operation or a campaign (FM 3-0). When large-scale combat operations commence, the joint force commander immediately exploits friendly capabilities across multiple domains and the information environment to gain the initiative.

4-2. The geographic combatant commander may direct a field army, corps, or division to establish a joint task force. In most cases, standing up a joint task force headquarters requires augmentation. Establishment of a joint network operations control center supporting the joint task force requires augmentation, either from other Services or elements of the theater tactical signal brigade. The joint task force J-6 determines communications requirements for the joint task force headquarters and lower echelon units directly supporting the commander, joint task force. Requests for support route through the geographic combatant command J-3 to the Joint Staff.

4-3. Establishing a joint task force to conduct large-scale combat operations requires speed, detailed planning, and coordination. The joint task force may use the facilities and assigned signal Soldiers of the theater or field army to support the joint task force headquarters until adequate facilities become available. The geographic combatant commander may attach elements of the theater tactical signal brigade to meet joint task force communications requirements until further augmentation or rotational units arrive.

RISKS TO SIGNAL SUPPORT

4-4. The enemy will seek to render U.S. combat power ineffective by systemic and continual attacks across multiple domains and the information environment, both before and during combat operations. These attacks include lethal attacks, cyberspace attacks, and electronic attacks targeting command and control nodes and networks. The isolation or destruction of a key command and control node offers the enemy a marked tactical advantage.

4-5. Commanders should assume the enemy considers the network and the ability to communicate to be key targets for destruction or degradation. Disrupting a unit's ability to communicate reduces its effectiveness and combat capability. The enemy can conduct electronic attacks to jam satellite positioning, navigation, and timing systems and degrade the effectiveness of precision munitions, sensor-to-shooter links, and navigation. The enemy may also use lethal fires, electronic attack, or cyberspace attack to destroy, degrade, disrupt, or isolate individual units and capabilities.

4-6. Peer threats may use EW capabilities before and during large-scale combat to locate and identify friendly command and control and other key nodes. Spectrum managers and EW personnel develop electronic

protection plans to reduce or mask the electromagnetic signature of the unit's command posts. Refer to FM 3-12, ATP 6-02.53, and ATP 6-02.70 for more information about electronic protection tasks.

SIGNAL SUPPORT

4-7. Army communications capabilities can support any joint or multinational combined arms team. Signal elements provide a wide variety of fixed and tactical communications capabilities to support a theater of operations.

4-8. Large-scale combat operations are lethal and complex. The full range of strategic to tactical signal capabilities support the combination of offense, defense, and stability tasks to seize, retain, and exploit the initiative, consolidate gains, win, and return to shaping operations. Large-scale combat operations require adaptable and agile communications support able to meet the specific mission requirements. Commanders can tailor employment of their communications capabilities to support their mission requirements, considering terrain, electromagnetic spectrum and satellite availability, and speed of displacement.

SIGNAL SUPPORT TO STABILITY TASKS

4-9. Stability tasks during large-scale combat operations include restoring essential services and population control in areas controlled by friendly forces. Generally, the responsibility for providing for the needs of the civilian population rests with the host-nation government or designated civil authorities, agencies, and organizations. Army forces perform the minimal essential stability tasks to provide security, food, water, shelter, and medical treatment when there is no legitimate civil authority or capability present. Army signal support may include emergency communications restoral to support stability tasks until host-nation civilian capabilities can be restored.

4-10. Functional support brigades, such as military police, engineers, and medical brigades, require communications augmentation when they support large-scale combat operations. Divisions also require network support for company- and platoon-level units performing stability missions. Elements of the expeditionary signal battalion support these requirements.

SIGNAL SUPPORT IN THE CORPS AND DIVISION SUPPORT AND CONSOLIDATION AREAS

4-11. A maneuver enhancement brigade typically controls and defends the corps or division support area. A brigade combat team controls and defends the consolidation area. Elements of the expeditionary signal battalion augment the maneuver enhancement brigade and brigade combat team's organic communications capabilities to establish the base communications network.

4-12. Perimeter defense forces, quick reaction forces, and roving guards primarily use single-channel radios for communications support. Units' organic and augmenting network capabilities support command posts for base security and defense. If base camps become enduring requirements, the base network migrates to a more permanent or fixed infrastructure. Fixed infrastructure frees tactical signal elements to support maneuver tasks.

SIGNAL SUPPORT TO TACTICAL ENABLING TASKS

4-13. Commanders direct tactical enabling tasks to support the performance of all offensive, defensive, and stability tasks. Commanders usually employ tactical enabling tasks as part of shaping operations or supporting efforts. The tactical enabling tasks are—

- Reconnaissance.
- Security.
- Troop movement.
- Relief in place.
- Passage of lines.
- Encirclement operations.
- Mobility and counter-mobility operations.

4-14. Large command post communications systems lack the mobility required during tactical enabling tasks. When executing tactical enabling tasks beyond the range of VHF single-channel radios, or when terrain prevents line of sight communications, units can employ retransmission capabilities, single-channel HF radios, narrowband (single-channel) tactical satellite radios, tactical messaging, or secure satellite telephones for communications between units and command posts.

4-15. Employing a retransmission site requires deliberate mission planning before deploying the team. Planning factors for retransmission include—

- Units supported.
- Planned retransmission locations throughout the mission, including alternates, with line of sight analysis.
- Triggers for displacement to alternate locations.
- Primary and alternate frequencies.
- Frequencies for emergency contact—
  - Medical evacuation.
  - Command.
  - Nearest units.
- Time required to be on station and retransmitting for supported units.
- Route and site security requirements.
- Infiltration and exfiltration routes.
- Whether unmanned aircraft systems or other aerial retransmission capabilities can meet the requirement.
- Plan to communicate with the parent unit (for example, contact the higher unit every two hours with update).
- Resupply plan.
- Concealment of the site.
- Plans to mask or reduce the electromagnetic signature of the site.

4-16. Passage of lines is generally considered a higher-risk operation. The division may establish a command and control node such as a tactical command post at the passage point to enable communications between passing units and their higher headquarters.

4-17. Relief in place operations require greater access to networked DODIN-A services than other maneuver tasks. Relief in place involves detailed planning and coordination between the current unit and the relief unit. The handover plan identify which communications systems rotate out with the departing unit and how to migrate services to the gaining unit's systems. The gaining unit generally retains the frequency allocations of the relieved unit, but deploys with its own allocated Internet protocol address range for its network and automated information systems.

SIGNAL SUPPORT TO FORCIBLE ENTRY OPERATIONS

4-18. Army signal forces must be capable of providing communications support from the point of departure, in transit, during landing, and throughout the fight to gain access to the geographic area controlled by hostile forces. Commanders and staffs must understand what communications capabilities and services will be available during each phase of the operation. Plans include the transition to more robust communications capabilities as they arrive in the area of operations. For example, during an airborne operation to seize an airfield, the aircraft may be fitted with wideband satellite communications capabilities to access video, imagery, databases, and e-mail while en route. During the airborne assault, communications are limited to single-channel radios. As the unit begins to consolidate gains, a small communications node may provide the commander, S-3, and S-2 with wideband satellite access to the DODIN-A. Once aircraft can land, the command receives and establishes its organic signal capabilities to support command post operations with wide-area network access.

SIGNAL SUPPORT IN THE TRANSITION TO CONSOLIDATE GAINS

4-19. Army forces provide the joint force commander the ability to capitalize on operational success by consolidating gains. Consolidation of gains is integral to winning armed conflict and achieving success across the range of military operations. Army forces consolidate gains in support of a host nation and its civilian population, or as part of the pacification of a hostile state.

4-20. During the consolidation of gains, signal units will see a rapid expansion in communications requirements. As the division establishes and expands the consolidation area, the division requires support from elements of the expeditionary signal battalion to support those augmenting units without organic signal capabilities. Requirements may include downward support to company and platoon echelons as the division establishes camps and bases to support operations to consolidate gains.

4-21. Depending on the enduring nature of camps and bases, the theater tactical signal brigade assists the corps and divisions by installing and transitioning to fixed strategic network infrastructure. Establishing fixed signal systems frees units' organic signal systems for follow-on operations while providing greater DODIN-A capacity and throughput.

SECTION II – LARGE-SCALE DEFENSIVE OPERATIONS

OVERVIEW OF LARGE-SCALE DEFENSIVE OPERATIONS

4-22. Army forces conduct defensive operations to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability tasks. There are three primary types of defensive operations:

- Area defense.
- Mobile defense.
- Retrograde.

4-23. The defense provides time for a commander to build combat power and establish conditions to transition to the offense. The inherent strengths of the defense include the defender's occupation of positions before an attack and the use of available time to prepare defenses. A defender maneuvers to place an enemy in a position of disadvantage and attacks the enemy at every opportunity using lethal fires, electronic attack, aviation, information-related capabilities, cyberspace operations, and obstacles, as well a joint assets.

SIGNAL SUPPORT

4-24. Signal support in large-scale defensive operations depends on the situation, terrain, and the primary defensive operation the Army force is executing. Signal leaders provide the communications capabilities required to support the mission. During planning for large-scale defensive operations, the Signal staff must ensure the commander understands what communications capabilities will be available at each critical point of the operation.

4-25. Signal support in large-scale defensive operations is critical to the Army winning. An accurate common operational picture helps commanders develop and share situational understanding to enable effective command and control. If forward observers cannot communicate with supporting fires elements, an enemy could penetrate the Army force's defense. In the mobile defense, the success of the strike force attacking at the decisive point and time relies on the timely and accurate flow of information. Signal soldiers must be operationally-focused and able to rapidly adapt to the constantly changing situation on the battlefield.

SIGNAL SUPPORT TO AREA DEFENSE

4-26. During the area defense, Army forces have the full array of their organic and augmenting communications systems to support the mission. Single-channel radio systems support mobile forces with retransmission sites positioned behind the main battle area, but capable of supporting primary and alternate defensive positions. Narrowband (single-channel) satellite or HF radios can be employed where terrain or

distance degrades or disrupts single-channel VHF communications. Units should rehearse the single-channel communications plan for the area defense and mitigate any challenges before the enemy attacks.

4-27. Signal nodes support each command post location and provide on-the-move wideband satellite communications to enable command and control on-the-move. Key command and control nodes should remain behind the main battle area, outside the range of cannon artillery. Units rehearse plans for battle handover and dislocation of command posts to mitigate the risk of the enemy locating and targeting friendly command and control nodes. Signal soldiers supporting command posts on the defense must train and rehearse command post displacement to reestablish communications as quickly as possible. The communications staff should work closely with the G-3 (S-3) when planning future command post locations to mitigate adverse effects of terrain and structures on the unit's communications capabilities.

4-28. If friendly communications nodes face imminent risk of being overrun, operators must evacuate COMSEC material and encryption devices or destroy them in place. Allowing COMSEC materials to fall into enemy hands compromises secure communications. COMSEC compromise disrupts all radio and data networks until operators and net control stations can conduct emergency cryptographic key supersession. Leaders must ensure all personnel train and rehearse these procedures as battle drills to prevent and mitigate COMSEC compromise.

SIGNAL SUPPORT TO MOBILE DEFENSE

4-29. A mobile defense is typically conducted when the terrain favors the attacker and there is sufficient depth to employ a striking force forward of the no penetration line (FM 3-0). The mobile defense consists of a fixing force, a striking force, and a reserve force.

4-30. Signal support to an Army force conducting a mobile defense is similar to that for an area defense. However, command posts forward of the no penetration line will likely rely on mobile communications capabilities such as single-channel radios and wideband on-the-move capabilities. Command and control nodes behind the no penetration line have full DISN services, but must be prepared to displace to mitigate the risk of being located and attacked.

4-31. Retransmission sites supporting the mobile defense should colocate with other Army elements if possible. If the retransmission site operates remotely, the site requires security augmentation. For retransmission planning considerations, see paragraph 4-15.

SIGNAL SUPPORT TO RETROGRADE TASKS

4-32. The *retrograde* is a defensive task that involves organized movement away from the enemy (ADP 3-90). Army units do not conduct the retrograde in isolation. Retrograde is part of a larger scheme of maneuver designed to regain the initiative and defeat the enemy. The three forms of retrograde are delay, withdrawal, and retirement.

4-33. Retrograde operations are some of the most demanding ground combat operations and rely heavily on mobile communications support. Similar to the support during mobile defense, single-channel VHF radios are the primary communications capabilities to support a delaying, withdrawing, or retiring force. HF and narrowband (single-channel) satellite radios are alternate means of communications when terrain or distance challenge line of sight radio capabilities. Retransmission systems extend the range of single-channel radio networks to support command and control in retrograde operations. For retransmission planning considerations, see paragraph 4-15. The constant movement of the retrograde force requires multiple planned retransmission site locations with routes that support quick dislocation and reestablishment to support the maneuvering force. Retransmission teams must track the progress of the operation to maintain awareness of supported force locations and when the operation meets a trigger to move to the next location. Units conducting retrograde operations usually deploy command and control nodes to the support area to establish the main command post ahead of the retrograde force and a tactical command post maneuvering with the main body.

RISKS TO SIGNAL SUPPORT

4-34. Peer threats will use EW capabilities to identify and locate friendly command and control nodes. Defending units should limit their electromagnetic emissions to protect networked systems and the integrity of data on those systems. Defenders can use terrain to mask emitters and reduce the probability of enemy signals intelligence and EW detection. Operating emitters remotely from command posts can increase command post survivability in case of detection and targeting. Refer to ATP 3-12.3 for techniques to reduce command post electromagnetic signature.

SECTION III – LARGE-SCALE OFFENSIVE OPERATIONS

4-35. Against a capable, adaptive enemy, the offense is the most direct and sure means of seizing, retaining, and exploiting the initiative to gain physical, temporal, and cognitive advantages and achieve definitive results (FM 3-0). Characteristics of the offense include audacity, concentration, surprise, and tempo.

OVERVIEW OF LARGE SCALE OFFENSIVE OPERATIONS

4-36. Army forces conduct offensive operations to defeat and destroy enemy forces and seize terrain, resources, and population centers. Effective performance of offensive operations capitalizes on accurate and timely communication of intelligence and other relevant information regarding enemy forces, weather, and terrain. There are four primary types of offensive operations:

- Movement to contact.
- Attack.
- Exploitation.
- Pursuit.

4-37. The overall concept for signal support is similar among all offensive operations. The specific tasks influence planning for signal support to each of these tasks in large-scale offensive operations.

SIGNAL SUPPORT

4-38. Corps and division commanders must be able to communicate with adjacent units, subordinates, supporting joint forces, and host-nation and multinational forces. Signal support allows command post personnel to access the full range of DODIN-A services and capabilities. Signal support is critical to transmit plans, develop common situational understanding, and to direct action to break the will of or destroy the enemy.

OPERATION IRAQI FREEDOM

On 19 March 2003, 3ID began its attack on Baghdad as the geographic combatant commander's main effort of OPERATION IRAQI FREEDOM. Because of the Army's lack of multi-channel tactical satellite ground systems and the time required to establish terrestrial based, line of sight networks, there were only two complete 24-hour periods when the network was available for the command. 3ID fought most of the war with the division command net on single-channel satellite radios and all other command communications on single-channel VHF radios. The United States declared victory on 14 April 2003 with the fall of Baghdad.

Since the conclusion of OPERATION IRAQI FREEDOM, the Army has transitioned its tactical communications capabilities to a primarily satellite-based, at-the-halt network with wideband line of sight radios to make the network more robust. Divisions and brigade combat teams have organic on-the-move network capabilities to quickly establish an agile network. This provides maneuver forces voice, data, and video capabilities on-the-move, and greater network throughput at-the-quick-halt.

4-39. Large-scale offensive operations are inherently mobile. Maneuver elements will perform tactical enabling tasks away from the command posts using highly mobile means of communications. The brigade combat team command posts maintain upper tier tactical internet connectivity for communications to division, but communication with subordinate echelons relies heavily on vehicle-mounted, man-pack, and handheld communications devices. When satellite transport is available, on-the-move networking provides improved situational awareness and increases the communications capabilities available at the battalion.

4-40. During planning and mission rehearsals, the S-6 staff must ensure the commander and staff understand the communications plan, specifically what communications capabilities will be available by phase of the operation or critical points of the battle. Command post personnel and their signal support must plan and rehearse rapid displacement to enhance command post survivability and support the rapid advance of maneuver forces.

4-41. Single-channel radio retransmission is a critical command and control enabler. Because U.S. ground forces move rapidly in offensive operations and the battlefield situation is fluid, retransmission teams must track the progress of the maneuver operation and anticipate emerging communications requirements. This awareness helps them maintain fully operational networks to support the commander's mission requirements. For retransmission planning considerations, see paragraph 4-15.

4-42. Signal elements support command and control as commanders maneuver their forces to positions of relative advantage before contact. Redundant systems and diversity in the network architecture allow for communications throughout the corps and division areas of operations. Although commanders require communications capabilities, effective command and control does not necessarily rely on continuous access to the DODIN-A. The commander's intent is the basis for all offensive operations. PACE plans, organic unit liaison teams, and digital liaison detachments provide commanders options to enhance coordination and interoperability. Units must train and rehearse to operate by redundant means and exercise disciplined initiative within the commander's intent when disconnected from the network.

SIGNAL SUPPORT TO SUSTAINMENT

4-43. Sustainment is critical to offensive operations. Sustainment units require reliable communications to control their teams operating from dispersed locations. Supply points, maintenance collection points, ambulance exchange points, and long-haul convoys are essential to mission success and operate throughout the corps and division areas of operations.

4-44. Long lines of communications may expand support area communications requirements beyond the organic signal capabilities of sustainment units. Dispersed sustainment nodes require expeditionary signal

battalion augmentation down to company level and some platoons to support the higher data throughput requirements for logistics support to offensive operations.

SIGNAL SUPPORT TO ENABLING UNITS

4-45. The theater tactical signal brigade and expeditionary signal battalions support corps and division enabling units that have no organic signal capabilities. Battalion and below units primarily communicate using single-channel radios in the offense. This results in fewer augmentation requirements at these echelons. Expeditionary signal battalions provide communications support to enabling units' command posts as they consolidate gains or transition to stability tasks. Expeditionary signal battalions also deploy teams and signal systems to replace battlefield losses, when directed.

RISKS TO SIGNAL SUPPORT

4-46. While Army forces conduct large-scale offensive operations, peer threats will use EW systems to identify and locate friendly command and control nodes. Units in the offense must limit electromagnetic emissions to protect mission command information systems and the integrity of data on those systems. Units use terrain to mask electromagnetic emissions and reduce the likelihood an enemy can locate and exploit command and control nodes. Locating antennas away from the command post enhances the survivability of the command post in case of detection. The cyber electronic warfare officer can develop plans to mask or reduce the radio frequency signature of signal systems. Refer to FM 3-12 and ATP 3-12.3 for more information on electronic protection techniques.

4-47. Satellite communications systems provide vital command post support and command and control on-the-move capabilities. However, when facing a peer threat with satellite denial capability, commanders must be prepared to fight and win with single-channel radio communications.

CONSOLIDATION OF GAINS

4-48. As the corps and divisions begin to transition from large-scale offense to area security and stability tasks, communications support must rapidly adapt from supporting maneuver operations to area support. Transition to consolidation of gains requires prior planning. Equipment and personnel must rapidly flow forward to establish fixed network infrastructure to support bases. Fixed infrastructure frees units' organic tactical communications systems for follow-on operations.

Chapter 5
Operations to Consolidate Gains

This chapter discusses signal support to Army operations to consolidate gains.

OVERVIEW OF OPERATIONS TO CONSOLIDATE GAINS

5-1. Commanders and staffs continuously consider activities necessary to consolidate gains and achieve the desired end state. Army units must consolidate gains to achieve enduring success. Consolidation of gains occurs in portions of an area of operations where large-scale combat operations are no longer occurring. Consolidation of gains consists of security and stability tasks and will likely involve combat operations against bypassed enemy forces and remnants of defeated units (FM 3-0). Army forces conduct consolidation of gains across the range of military operations. Consolidation of gains makes military objectives enduring.

5-2. During large-scale combat operations, the size of consolidation areas generally increases as the operation progresses and units achieve combat successes. Eventually, most Army units can expect to conduct some consolidate gains activities during large-scale combat operations.

5-3. During operations to consolidate gains, Army and joint commanders must be able to—

- Employ joint fires.
- Manage airspace.
- Conduct sustainment tasks.
- Conduct security tasks.
- Begin reconstruction.
- Coordinate humanitarian relief.

SIGNAL SUPPORT

5-4. Operations to consolidate gains change the focus of signal support. The corps and division G-6 staffs and the theater tactical signal brigade refine plans to transition available signal capabilities to support consolidation areas.

5-5. During operations to consolidate gains, communications requirements will quickly surpass the capabilities of single-channel radio communications. The expeditionary signal battalion's downward support requirements increase significantly as company- and platoon-sized units conduct area security and other consolidate gains tasks.

5-6. Tactical signal units may support communications requirements for local and area security, civil security and control, restoration of essential services, and security cooperation. Expeditionary signal units provide this support only until civilian, local government or other agencies can establish communications. The transfer of an area of operations to legitimate civil authorities relieves the land force of area security and stability tasks and represents a transition from operations to consolidate gains to operations to shape or prevent. Regardless of the tasks required in a specific area of operations, signal units support the Army's strategic roles of shape, prevent, win, and consolidate gains.

5-7. During operations to consolidate gains, expeditionary signal capabilities return to their parent commands as soon as fixed communications infrastructure is available to support enduring base requirements. Strategic satellite and terrestrial network transport capabilities provide high-throughput connections to the DODIN-A. DODIN operations and cybersecurity tasks transition from the brigade combat team and division to the corps, theater army, theater tactical signal brigade, and SC(T).

RISKS TO SIGNAL SUPPORT

5-8. An enemy may continue to direct information warfare activities, including cyberspace and EW attacks, to disrupt U.S. communications and prevent consolidation of gains. Enemy forces will likely continue to fight even after friendly forces attain their initial military objectives in the close area.

5-9. Some enemy formations may be intentionally or unintentionally bypassed during close operations as friendly forces focus on the decisive effort. As U.S. forces attempt to consolidate gains, command posts and signal sites are vulnerable to physical attack from bypassed conventional and irregular forces.

Appendix A

Operating 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 EW and cyberspace attacks.

THREAT TACTICS, TECHNIQUES, AND PROCEDURES

A-1. Information and its management, dissemination, and control have always been critical to the successful conduct of tactical missions. Given today's advancements in information and information systems technology, this importance is growing in scope, impact, and sophistication. The opposing force recognizes the unique opportunities that information warfare gives tactical commanders, and it continuously strives to incorporate information warfare activities in all tactical missions and battles (TC 7-100.2).

A-2. 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-3. 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.

A-4. Commanders, their staffs, and equipment operators must train to recognize and react to peer threat information warfare tactics, techniques, and procedures if they are to continue communicating in a contested environment.

U.S. MEASURES TO PREVENT THREAT EFFECTS

A-5. There are operational tactics, techniques, and procedures signal planners and operators can take to mitigate peer threat capabilities in the electromagnetic spectrum. If an enemy cannot detect friendly signals, they cannot geolocate or jam those signals.

LIMITING ELECTROMAGNETIC SIGNATURE

A-6. 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 site selection for communications equipment.
- Employment of directional antennas.
- Operations using the lowest power required.
- Limiting radio transmissions.
- Using burst transmission to minimize transmission time.
- Using a random battle rhythm schedule.

A-7. Electronic protection techniques can also help mask the electromagnetic signature of command posts and communications sites. The cyber electronic warfare officer assists the G-6 (S-6) in planning electronic protection measures to reduce the command post signature.

Terrain Masking

A-8. 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-9. Radar reflective camouflage netting is an effective means of blocking unintended electromagnetic radiation from the rear and sides of directional antennas. Camouflage netting to the sides and back of a line of sight or satellite communications antenna ensures only the main beam of the antenna radiates. This main beam is highly directional; it is much harder to detect since the enemy would need to be directly in the transmission path.

Line of Sight

A-10. High-throughput line of sight radios can carry high bandwidth data over distances up to 25 miles, but the links need to be engineered to minimize the chance of detection, targeting, and jamming. If the line of sight path is parallel to the forward line of troops, an enemy is less likely to detect the signal, and enemy jammers will be unable to reach the antenna with a signal strong enough to jam the radio.

REMOTE ANTENNAS

A-11. Large command posts and their high-throughput communications systems emit a significant amount of electromagnetic energy. While planners and operators can mask some of this energy with careful siting, terrain masking, and directional antennas, some electromagnetic energy remains. Because peer threats target friendly command and control capabilities, anything near the communications system is at risk of destruction from lethal fires.

A-12. Commanders and signal planners should consider locating major communications assemblages as far from the supported command post as practical. Placing terrain features, man-made structures, or distance between communications systems and command posts provides the command post protection 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-13. Despite all efforts to reduce and mask the electromagnetic signature of a command post, a peer threat is likely to locate it eventually. Moving a command post frequently reduces the chances of destruction. Frequent moves are especially important when operating within the range of enemy artillery.

A-14. 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.

INTEGRATION WITH OTHER STAFF ELEMENTS

A-15. The G-6 (S-6) cannot plan signal support alone. Other staff sections' functions and capabilities help inform sound, survivable signal support plans. Staff sections activities during the military decision-making process reinforce each other's planning efforts.

A-16. The cyber electronic warfare officer, signal planners, spectrum managers, and the G-2 (S-2) assess threats to friendly communications during the military decision-making process. Integrated planning counters

enemy attempts to exploit vulnerabilities of friendly communications systems. When creating electronic protection plan, the cyber electronic warfare officer and signal planners consider deployment, employment, replacement, and concealment of communications systems.

Cyberspace Electromagnetic Activities Section

A-17. The CEMA section of the G-3 (S-3) from brigade to corps coordinates and synchronizes cyberspace and EW operations for effective collaboration across staff elements. This section includes the cyber electronic warfare officer, the spectrum manager, the EW technician, and EW noncommissioned officers. The CEMA section is key to the collaboration of cyberspace and EW operations. The cyber electronic warfare officer is the cyberspace planner and understands the operations and missions of the unit and the commander's intent. The CEMA section participates in the planning and targeting process, and leads the CEMA working group to support the military decision-making process. The cyberspace planner submits requests for effects provided by non-organic resources. Other key staff members who assist in CEMA include the G-2 (S-2), G-3 (S-3), G-6 (S-6), supported by the network operations and service center and signal company). CEMA Section activities include—

- Plans, requests, and synchronizes effects in cyberspace and the electromagnetic spectrum to support freedom of maneuver.
- Coordinates with higher headquarters staff to integrate and synchronize information collection efforts to support cyberspace and EW operations.
- Synchronizes cyberspace and EW effects requests with organic targeting capabilities.
- Prepares and submits effect requests using the cyber effects request format or electronic attack request format.
- Develops, maintains, and disseminates cyberspace and electromagnetic spectrum input for the common operational picture.
- Plans, coordinates, integrates, prepares for, and conducts EW operations.
- Conducts spectrum management coordination for EW capabilities within the unit's area of operations.
- Prepares and submits effect requests using the cyber effects request format, as required.
- Provide recommendations on commander's critical information requirements.

The G-6 (S-6)

A-18. The G-6 (S-6) section prepares annex H (Signal) to the operation plan or order, with appropriate cross-references to the EW portions of annex C (Operations), operations security portion of annex E (Protection), the military deception plan, and the signal operating instructions. The G-6 (S-6) integrates and coordinates DODIN operations and spectrum management operations through close collaboration with the CEMA section during planning and operations. The G-6 (S-6) also—

- Plans alternate means of communications for those systems most vulnerable to enemy jamming.
- Provides COMSEC to protect systems most vulnerable to enemy information gathering activities.
- Plans measures to protect critical friendly frequencies from intentional and unintentional electromagnetic interference.
- Enforces proper use of radio, electronic protection, and transmission security procedures on communications channels.
- Performs spectrum management, including designating alternate frequencies for radio networks and modeling the electromagnetic environment.
- Publishes and updates signal operating instructions.
- Prepares and maintains the restricted frequency list—taboo, protected, and guarded frequencies, in collaboration with the G-2 (S-2).
- Implements cybersecurity on the network and automated information systems.

The G-3 (S-3)

A-19. The G-3 (S-3) is the staff lead in planning and the conduct of Army operations. During the planning and execution of EW and signal support, the G-3 (S-3)—

- Exercises staff responsibility for electronic protection.
- Includes electronic warfare support and electronic attack scenarios in all command post and field training exercises.
- Evaluates electronic protection techniques employed.
- Includes electronic protection in the unit training program.

Cyber Electronic Warfare Officer

A-20. The cyber electronic warfare officer plans, coordinates, and directs the execution of EW activities. The cyber electronic warfare officer is also the lead for the CEMA section. The cyber electronic warfare officer—

- Serves as subject matter expert on enemy EW capabilities and EW rules of engagement.
- Leads the EW working group.
- Submits information requirements to the G-2 (S-2) to support EW planning and assessment.
- Supports the G-2 (S-2) during intelligence preparation of the battlefield.
- Coordinates with the G-6 (S-6) to plan, implement, and assess friendly electronic protection measures.
- Coordinates with the G-6 (S-6) spectrum manager to ensure planned EW activities do not interfere with friendly communications.
- Deconflicts EW operations with the spectrum manager in the CEMA section.
- Collaborates with the G-2 (S-2) to synchronize and deconflict EW operations with intelligence activities.

G-2 (S-2)

A-21. The G-2 (S-2) provides current intelligence estimates during the military decision-making process, and updated estimates during operations. The intelligence estimate includes—

- Current enemy tactics, techniques, and procedures.
- Enemy locations in relation to friendly forces.
- The enemy's electronic technical data—enemy capabilities that could be used to deny friendly use of the electromagnetic spectrum.
- Known cyberspace threats to inform cybersecurity and defensive cyberspace operations efforts.

RECOGNIZING AND RESPONDING TO THREAT EFFECTS

A-22. 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 personnel and leaders must learn to identify and respond to threat effects in cyberspace and the electromagnetic spectrum.

ELECTROMAGNETIC SPECTRUM (JAMMING)

A-23. *Electromagnetic jamming* is the deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, 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-24. 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.

Communications Jamming

A-25. 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-26. Radio operators must train to quickly differentiate between internal and external interference. Refer to ATP 6-02.53 for more information about isolating and eliminating internal sources of interference.

A-27. 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-28. 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-6 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-29. 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-30. 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-31. 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 they are ordered to do so. Operators should be careful not to disclose to the enemy that the radio has been adversely affected. This means normal operations should continue even when degraded by jamming.
- **Increasing transmitter power output.** Low power is used for normal operations to minimize 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 moving the antenna and associated radio set anywhere from a few meters to several hundred meters.
- **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 PACE plan.** Quickly changing to the alternate or contingency means of communications reduces communications disruption.
- **Using signals intelligence or EW capabilities to locate the jamming signal.** Leveraging signals intelligence or EW capabilities requires coordination and collaboration with the G-2 (S-2) or the cyber electronic warfare officer.

A-32. 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-33. 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-34. 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-35. 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-36. 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-37. 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 location is known, increased distance or terrain masking may mitigate interference.
- **Use signals intelligence or EW capabilities to locate the jamming signal.** Leveraging signals intelligence or EW capabilities requires coordination and collaboration with the 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-38. 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-39. 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-40. 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-41. 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 PACE plan.** Quickly changing to the alternate or contingency means of communications reduces communications disruption.
- **Use signals intelligence or EW capabilities to locate the jamming signal.** Leveraging signals intelligence or EW 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 will be unable to communicate beyond line of sight, or through significant physical obstacles.

A-42. 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-43. 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-44. Frequency managers and EW personnel attempt to resolve incidents at the lowest possible level using organic assets. If the spectrum manager and the 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-45. 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-46. 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-47. 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-48. Army units report through their chain of command up to the geographic combatant command, and to the U.S. 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-49. 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-50. 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-51. 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-52. 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-53. 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-54. 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 J-6 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-55. 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-56. 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-57. 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-58. 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 J-6.
- Continue operations using alternate or contingency communications means.
- Report to G-2 (S-2) and G-3 (S-3).

A-59. 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-60. 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. This compromise may place operations at risk.

A-61. 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-62. 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-63. 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-64. 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 operation or support plans become compromised.

Malware Attacks Against Combat Platforms

A-65. Many modern combat platforms rely heavily on embedded computer systems. Any computerized system is susceptible to malware injection in the logistics chain, during maintenance, or through corrupted or unauthorized software updates.

Preventive Measures

A-66. Strict physical security and cybersecurity controls can prevent most potential sources of malware injection. Maintainers prevent malware injection by—

- Verifying the source of all software updates.
- Checking the software hash to verify software has not been manipulated.
- Maintaining strict physical control of data storage devices and maintenance computer systems.
- Avoiding the unauthorized use of removable storage media, such as thumb drives.

Indicators

A-67. Possible indications of a malware attack against combat platforms include—

- Similar faults on multiple systems, either simultaneously or within a short period.
- Faults related to subcomponents that rely on embedded computers for operation.

Reaction

A-68. If equipment maintainers suspect compromised operating software on a combat platform, they should—

- Review maintenance records of software updates.
- Report incidents to G-2 (S-2) and G-3 (S-3).
- Report incidents to the next higher echelon.
- Roll back software updates to the last known good configuration, if possible.

Social Engineering

A-69. 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-70. 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-71. 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.

A-72. 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-73. Indicators of social engineering attempts include—

- Unexpected phone calls from unknown callers requesting sensitive information.
- Websites that do not look normal, have several broken links, or mismatching Internet address.
- Unauthorized personnel shoulder surfing.

Reaction

A-74. 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.

A-75. Promptly reporting attempts at social engineering can raise awareness and prevent others from falling victim to the same techniques.

Phishing and Spear Phishing

A-76. 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.

A-77. Any individual may fall victim to a phishing attack. Key leaders and network administrators are also subject to spear phishing.

Preventive Measures

A-78. 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-79. Most common phishing techniques share certain traits, including—

- E-mails with generic greetings. Note that spear phishing attempts are more sophisticated and address targeted individuals 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-80. 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.

A-81. Individuals can further protect themselves from fraudulent links by never accessing their personal accounts through links in e-mails. For instance, if an e-mail purports to be from the individual's bank or credit card company, they should access their account only through the legitimate secure website, not through a hyperlink provided in an e-mail.

A-82. Commands should not threaten punishment against personnel who inadvertently fall victim to phishing attempts. Fear of punishment could prevent individuals from reporting attacks.

Social Media Attacks

A-83. 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-84. 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-85. Individuals should restrict who can view their social media profile and activities using the privacy settings on the social media platform.

A-86. Individuals and public affairs personnel must carefully weigh operations security considerations when they engage on social media platforms.

A-87. Individuals and group administrators should not accept friend or group membership requests from unknown or unverifiable persons.

A-88. Commands should consider limiting or restricting access to social media platforms as mission or operations security concerns dictate.

Indicators

A-89. 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-90. If a social media attack is known or suspected, personnel should—

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

Attacks Against Personal Electronic Devices

A-91. 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 cell 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-92. 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.

A-93. Commanders should consider restricting or banning the use of personal electronic devices, based on the tactical situation.

Indicators

A-94. 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-95. If a unit suspects it has come under attack, they should—

- Quickly displace the element under attack and direct all personnel to immediately 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

Signal Planning

The G-6 (S-6) advises the commander and conducts planning and coordination for DODIN operations, network transport and information services, spectrum management, and COMSEC. Signal planners are subject matter experts in these areas, so they can formulate signal plans and evaluate the signal supportability of various courses of action during the military decision-making process.

MILITARY DECISION-MAKING PROCESS

B-1. The *military decision-making process* is an iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order (ADP 5-0). In simple terms, the military decision-making process is a systematic method to solve a specific military problem. During the planning and orders production process, G-6 (S-6) staff maintains the running signal staff estimate and plans the scheme of signal support to support the unit's operation.

SIGNAL STAFF ESTIMATE

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

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

B-3. The signal staff estimate outlines the G-6 (S-6) and assigned or supporting signal elements' ability to support various friendly courses of action. Signal planners evaluate the communications and network requirements for each proposed course of action and against the available signal support. Evaluating the available signal support includes considering the capabilities and limitations of supporting signal systems. An accurate running estimate is invaluable throughout the military decision-making process. If signal elements cannot support a proposed course of action, the running estimate should identify the shortfall. The signal staff estimate includes all relevant signal information, including a signal mission analysis chart, which outlines—

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

B-4. The staff derives the running estimate from facts, assumptions, and situational analysis (terrain, friendly situation, enemy situation, and support requirements). Signal planners use the running estimate through each step of the military decision-making process. Planners update the running estimate when—

- The commander and staff recognize new facts.
- The staff can replace assumptions with facts or find previous assumptions invalid.
- The mission changes.
- Planners receive updated information from other staff sections.

B-5. The staff adjusts the running estimate based on the course of action development and war-gaming. After course of action approval, the signal running estimate forms the basis for annex H (Signal) of the operation plan or order.

PRIMARY, ALTERNATE, CONTINGENCY, AND EMERGENCY PLAN

B-6. Building an effective PACE plan may be simultaneously the most useful and challenging practice for communications planners. The key to a good PACE plan is to establish redundancy, so some means of communication is always available. Signal leaders and planners must understand their organization's authorized and available communications capabilities and limitations, as well as the personnel and logistic requirements to employ and sustain the capabilities. During the military decision making process, G-6 (S-6) planners ensure proposed PACE plans are feasible, acceptable, suitable, distinguishable, and complete.

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

B-7. The PACE plan should be as simple as possible to support reliable communications during dynamic operations. If possible, PACE plans should revolve around warfighting functions. The principal warfighting functions for the purposes of PACE planning are movement and maneuver, intelligence, fires, and sustainment. The G-6 (S-6) does not dictate PACE plans for these warfighting functions, but does educate the warfighting function leads on available capabilities during operations and assists the warfighting function staff in formulating a PACE plan.

B-8. Planners should identify appropriate PACE systems for each phase—for example, defense, offense, or consolidating gains—and publish them in annex H (Signal) of the operation order. An emergency means of communications does not necessarily have to be equipment; it may be a procedure such as moving back to the last known effective communications point or rallying at a specified grid coordinate. The PACE plan helps ensure communications availability if the primary means of communication fails. Units should rehearse and validate the PACE plan during mission and communication rehearsals to ensure all personnel can execute the plan as necessary. Refer to ATP 6-0.5 for information about communication rehearsals. Table B-1 shows an example of a simple PACE plan for one phase of an operation, aligned with warfighting functions.

Table B-1. Example primary, alternate, contingency, and emergency communications plan by warfighting function

	Movement and Maneuver	***Intelligence***	***Fires***	***Sustainment***
Primary	VHF (CMD net)	VHF (O&I)	AFATDS	VHF (A&L)
Alternate	SC TACSAT	JBCP	VHF (voice)	JBCP
Contingency	JBCP	SC TACSAT (voice)	VHF (digital)	SC TACSAT (voice)
Emergency	HF (chat)	TIGR	JBCP	BCS3

Legend:

AFATDS	Advanced Field Artillery Tactical Data System	HF	high frequency
		JBCP	Joint Battle Command Platform
A&L	administrative and logistics	O&I	operations and intelligence
BCS3	Battle Command Sustainment and Support System	SC	single-channel
		TACSAT	tactical satellite
CMD	command	TIGR	tactical ground reporting
FM	frequency modulation	VHF	very high frequency

RECEIPT OF MISSION (STEP 1)

B-9. Commanders initiate the military decision-making process upon receipt, or in anticipation of, a mission. The signal staff coordinates with higher and adjacent headquarters staff counterparts to collect information on current and future signal support, running estimates, and other signal planning products. Planners collect—

- Paper and digital maps for the area of operations.
- Signal plans and annexes from higher headquarters.
- List of available signal equipment and personnel assets.
- Resource allocation—frequencies, satellite access, bandwidth, information services.
- Tactical standard operating procedure of the unit and higher headquarters.
- Reporting requirements.
- Cybersecurity procedures.
- COMSEC procedures.
- Applicable field and technical manuals.

B-10. On receiving a mission, G-6 (S-6) planners begin collaborating with higher, adjacent, and subordinate signal elements.

- **Higher.**
  - Confirm higher headquarters communications assets and requirements.
  - Higher headquarters network architecture, COMSEC, and spectrum management.
  - Retransmission locations for possible collocation.
  - Systems under operational management.
- **Adjacent.**
  - Retransmission locations for possible collocation.
  - Operational management of equipment, as directed.
  - Possibility of sharing signal assets.
- **Subordinate.**
  - Tasks required of subordinate elements.
  - Resources available to augment subordinate units' capabilities.
  - Assistance requesting outside augmentation, such as pooled theater resources.

B-11. During the receipt of mission step, planners prepare the initial signal estimate. Table B-2 on page B-4 identifies the key inputs, planning process, and key outputs for step 1.

Table B-2. The military decision-making process, step 1: receipt of mission

Key inputs	Process	Key outputs
Higher headquarters plan or order. Planning products from higher headquarters, including the signal annex (annex H)	Begin updating the signal running estimate. Gather tools to prepare for mission analysis specific to signal support. Provide signal input for formulation of the commander's initial guidance and warning order.	Initial signal running estimate.

MISSION ANALYSIS (STEP 2)

B-12. Mission analysis is the method for clearly identifying a problem and the tools available to solve it. Commanders and their staffs conduct mission analysis to develop their understanding of the situation and problem, identify what the command must accomplish, when and where it must be done, and why. The signal staff gathers, analyzes, and synthesizes information on the current conditions of the operational environment with an emphasis on signal support, spectrum management operations, and the information environment. At this point, planners identify any restraints imposed by signal systems in the intended operational environment.

B-13. Planning using the Army design methodology may occur before the military decision-making process, take place concurrently with the military decision-making process, or might not be conducted at all. The commander and staff should review Army design products, if available, to enhance situational understanding and integrate them into the military decision-making process.

B-14. Intelligence support to signal begins with intelligence preparation of the battlefield and continues throughout the operations process. *Intelligence preparation of the battlefield* is the systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations (ATP 2-01.3). The signal staff and CEMA section coordinate with the G-2 (S-2) staff to identify enemy and adversary capabilities and help develop models, situation templates, event templates, high-value targets, named areas of interest, and other outputs from the intelligence process, including enemy and adversary cyberspace, EW, and communications information.

B-15. The signal staff identifies—

- Facts and assumptions (what planners know and what they assume to be true about the operation, operational area, and enemy).
- Tasks.
  - Specified.
  - Implied.
  - Essential.
- Planning constraints—what the unit must do.
- Planning restraints—what the unit cannot do.
- Risks.

B-16. Some information from the higher headquarters order, if it is available, establishes the basis for developing the signal plan. The G-6 (S-6) should extract—

- Task organization.
- Reporting requirements.
- Higher headquarters communications support and architecture.
- Enemy command and control capabilities and threat.

- Higher headquarters' execution timeline.
- COMSEC key, period change, and compromise procedures.
- Cybersecurity requirements.
- Scheduled network outages.
- Signal tasks—
  - Specified.
  - Implied.
  - Essential.

B-17. The G-6 (S-6) considers these facts and assumptions:

- Maintenance status of communications equipment and systems.
- Technical limitations of equipment—range, weather, and bandwidth.
- Areas of limited communications coverage.
- Higher headquarters support—
  - Services.
  - Bandwidth.
  - Frequencies.
- Personnel status.
- Effects of the operational environment on communications.
- Threat intelligence and EW capabilities.
- COMSEC changes.
- Command post locations.
- Security of isolated or moving communications nodes.
- Communications requirements of attached units.

B-18. The G-6 (S-6) nominates commander's critical information requirements and essential elements of friendly information related to signal support. During mission analysis, the G-6 (S-6) conducts signal site analysis (see paragraph A-51) to identify the most effective operating locations and updates the running estimate. The G-6 (S-6) begins collaboration with the G-3 (S-3), G-2 (S-2), and sustainment staff sections. This collaboration continues throughout the planning process. Table B-3 on page B-6 identifies the key inputs, planning process, and key outputs for step 2.

Table B-3. The military decision-making process, step 2: mission analysis

Key inputs	Process	Key outputs
Commander's initial guidance. Army design methodology product. Higher headquarters plan or order.	Analyze inputs and develop information requirements. Participate in intelligence preparation of the battlefield. Determine signal specified and implied tasks. Determine signal limitations and constraints. Identify critical facts and assumptions. Identify and nominate signal-related commander's critical information requirements. Identify and nominate signal essential elements of friendly information. Provide signal input to the combined information overlay. Provide signal input for development of mission analysis brief and warning order. Participate in mission analysis brief.	List of signal information requirements. Overlays from intelligence preparation of the battlefield process to support signal operation. List of signal specified and implied tasks. List of signal limitations and constraints. List of signal facts and assumptions. Updated signal running estimate.

COURSE OF ACTION DEVELOPMENT (STEP 3)

B-19. Course of action development is the method to determine the best employment of the tools available to solve the problem identified in mission analysis. Course of action development generates options for subsequent analysis and comparison to satisfy the commander's intent and planning guidance. The G-3 (S-3) staff usually drives course of action development, aided by the subject matter expertise of the other staff sections. The signal staff applies the knowledge gained from the mission analysis step to help develop proposed courses of action. During course of action development, the signal staff develops a draft scheme of signal support. The scheme of signal support describes how the commander intends to use organic and augmenting signal assets to support the concept of operations, with an emphasis on the scheme of maneuver.

B-20. The G-6 (S-6) understanding of the operating characteristics and limitations of the unit's communications systems helps the G-3 (S-3) develop feasible courses of action. Lack of reliable communications could render an otherwise promising course of action unsupportable.

B-21. The staff typically develops two to three proposed courses of action for comparison. Each course of action must be—

- **Complete.** The proposed course of action can accomplish the mission within available time, space, and resources.

- **Feasible.** The unit has the capacity to accomplish the mission within available time, space, and resources.
- **Acceptable.** The tactical or operational advantage gained by executing the course of action justifies its resource cost, especially in casualties.
- **Distinguishable.** The proposed course of action differs identifiably from the others.
- **Suitable.** The proposed course of action can accomplish the mission and comply with the commander's guidance.

Note. While each course of action must meet all five criteria, the communications plan does not necessarily have to be distinguishable. One communications plan may support multiple courses of action.

B-22. For each proposed course of action, the signal staff identifies the PACE plan for each phase of the operation. Planners establish the communications plan to support each phase. The communications plan includes—

- Long-haul communications.
- Combat net radios and retransmission.
- Network transport.
- Line of sight analysis.
- Triggers for movement of command and control nodes and systems, include primary and alternate routes and locations, and time and space required for movement.

B-23. The staff bases signal support priorities on the commander's guidance for priority of effort:

- Weighting the main effort.
- Sufficient redundancy for key command and control nodes—the tactical command post and command group—at critical times.

B-24. The G-6 (S-6) recommends command post locations based on communications requirements, equipment operating characteristics, and the tactical situation. Through course of action development, planners formulate a clear concept of signal support for each proposed course of action with an understanding of which command post is controlling the fight by phase of the operation. The concept of signal support includes necessary support tasks performed by non-signal personnel, such as quick reaction force, security, and casualty evacuation.

B-25. On completion of course of action development, many outputs from the mission analysis may require updates, such as signal-related input for the commander's critical information requirements and essential elements of friendly information. The signal staff updates their portions of the draft operation order, including annex H appendixes with signal support information. Table B-4 on page B-8 identifies the key inputs, planning process, and key outputs for step 3.

Table B-4. The military decision-making process, step 3: course of action development

Key inputs	Process	Key outputs
Commander's initial guidance. Initial commander's critical information requirements. Updated intelligence preparation of the battlefield products. List of specified and implied signal tasks. List of signal limitations and constraints. List of signal facts and assumptions. Updated signal running estimate.	Identify signal vulnerabilities of friendly and neutral actors. Provide signal input for the combined information overlay. Determine the initial scheme of signal support. Provide signal input for the course of action development brief. Begin development of annex H (Signal) to the operation order.	Updated list of signal information requirements. Draft scheme of signal support. Updated signal running estimate.

COURSE OF ACTION ANALYSIS (STEP 4)

B-26. Course of action analysis enables commanders and staffs to identify difficulties, coordination problems, and the probable consequences of each course of action considered. As the staff war-games proposed courses of action, the G-6 (S-6) assesses DODIN operations, spectrum management operations, cybersecurity, and information protection feasibility. The G-6 (S-6) defines communications systems requirements, compares them to available assets (organic and attached), identifies potential shortfalls, and recommends actions to eliminate or reduce their effects.

B-27. When determining feasibility and supportability of proposed courses of action, the G-6 (S-6) evaluates potential signal sites. The signal site must be defensible, and the location must not interfere with the operation of signal equipment. For example, structures or terrain do not block line of sight between a satellite communications terminal and the orbiting satellite.

B-28. As the staff war-games proposed courses of action, the G-6 (S-6) provides signal input, including—

- Movement of command and control nodes.
- Emplacement of network architecture, network transport, and retransmission nodes.
- Command and control synchronization and execution matrix.

B-29. The G-6 (S-6) evaluates the feasibility of the communications plan for each proposed course of action, including the communications advantages, disadvantages, and recommended solutions for communications disadvantages. Upon completion of course of action analysis, operational planning continues with updating the commander's critical information requirements and signal running estimate. The signal staff refines their scheme of signal support, ensuring that it nests with and supports the scheme of maneuver. Table B-5 on page B-9 identifies the key inputs, planning process, and key outputs for step 4.

Table B-5. The military decision-making process, step 4: course of action analysis

Key inputs	Process	Key outputs
Revised commander's planning guidance. Draft scheme of signal support. Updated signal running estimate.	Provide signal input and participate in the war-game briefing, as required. Integrate and synchronize signal support into the scheme of maneuver and concept of operations. Continue developing scheme of signal support. Provide signal input for the development of the decision support matrix and decision support template. Provide refined signal support input to the combined information overlay.	Refined signal input to the commander's critical information requirements. Refined scheme of signal support. Updated signal running estimate.

COURSE OF ACTION COMPARISON (STEP 5)

B-30. Course of action comparison is a process to evaluate proposed courses of action against objective evaluation criteria approved by the commander and staff. During course of action comparison, all staff sections analyze and evaluate the advantages and disadvantages of each proposed course of action from their perspective. The G-6 (S-6) section may not directly participate in this process. The G-3 (S-3) usually conducts course of action comparison based on principles of warfare, doctrinal fundamentals, or the commander's guidance and intent. The G-6 (S-6) should ensure the available signal assets are adequate to support each course of action, and there is adequate security and defense for the number of signal sites required. During course of action comparison, the G-6 (S-6) recommends a concept of signal support for each course of action and provides supporting criteria:

- Simplicity of the communications plan.
- Coverage of combat net radio networks.
- Number of command and control node movements required.
- Timeline of information services availability.

B-31. After course of action comparison, output products and the base operation order enter final draft. Table B-6 on page B-10 identifies the key inputs, planning process, and key outputs for step 5.

Table B-6. The military decision-making process, step 5: course of action comparison

Key inputs	Process	Key outputs
War-game results. Refined scheme of signal support. Updated signal running estimate.	Analyze advantages and disadvantages of each proposed course of action. Provide signal input to the decision matrix tool, as required. Provide signal input for the risk assessment. Develop recommendation for the most supportable course of action from a signal support perspective. Provide signal input for development of the course of action comparison briefing, as required.	Recommended concept of signal support. Updated signal running estimate.

COURSE OF ACTION APPROVAL (STEP 6)

B-32. During course of action approval, the commander selects the most advantageous course of action to accomplish the mission. The selected course of action must first be ethical, and then the most effective and efficient possible. During the course of action approval briefing, the G-6 (S-6) briefs the commander on the signal support plan for each course of action, including the advantages or disadvantages of each. The G-6 (S-6) should be able to articulate whether and why the recommended course of action is more supportable than the alternatives. The commander issues final planning guidance, including a refined commander's intent, the commander's critical information requirements, and any additional guidance on warfighting function priorities. Table B-7 on page B-11 identifies the key inputs, planning process, and key outputs for step 6.

Table B-7. The military decision-making process, step 6: course of action approval

Key inputs	Process	Key outputs
Updated signal running estimate, including refined products for each proposed course of action. Evaluated courses of action. Recommended course of action.	Receive and respond to final planning guidance from commander. Assess implications and revise relevant portions of the operation order. Finalize scheme of signal support.	Commander-approved course of action. Final draft for relevant portions of paragraph 5, command and signal, to the operation order. Final draft annex H (Signal) to the operation order. Final draft signal input to appendix 1 (Defensive Cyberspace Operations) to annex H (Signal). Final draft appendix 2 (Network Operations) to annex H (Signal). Final draft appendix 3 (Network Diagrams) to annex H (Signal) Final draft appendix 4 (Satellite Communications) to annex H (Signal). Final draft appendix 5 (Foreign Data Exchanges) to annex H (Signal). Final draft appendix 6 (Spectrum Management) to annex H (Signal). Final draft appendix 7 (Information Services) to annex H (Signal). Final draft signal input to annex B (Intelligence).

ORDERS PRODUCTION, DISSEMINATION, AND TRANSITION (STEP 7)

B-33. The final step of the military decision-making process is orders production, dissemination, and transition. The staff prepares the operation order by turning the selected course of action into a clear, concise concept of operations with supporting information, as required. The signal staff finalizes all planning products, including the signal running estimate and annex H of the operation order (with appendixes). If time allows, the staff can conduct a more thorough war game of the approved course of action. The staff internally reconciles planning outputs for approval by the commander.

B-34. The G-6 (S-6) staff prepares annex H (Signal) and its appendixes. The G-6 (S-6) staff also collaborates with the G-3 (S-3) to prepare appendix 12 (Cyberspace Electromagnetic Activities) to annex C (Operations), with input from the G-2 (S-2) staff.

B-35. The phases in the scheme of signal support match the phases of the base plan or order. The scheme of signal support outlines the priorities of support for each phase of the operation.

B-36. Because there is often little time between course of action approval, the operation order brief, and orders production, it is useful for the signal staff to maintain a signal annex template. Using a template speeds up order production, since most recurring information pre-populates the appropriate paragraphs. The higher headquarters plan or order can also provide a useful framework. Table B-8 identifies the key inputs, planning process, and key outputs for step 7.

Table B-8. The military decision-making process, step 7: orders production, dissemination, and transition

Key inputs	Process	Key outputs
Commander-approved course of action and any modifications.	Participate in staff plans and orders reconciliation, as required.	Relevant portions of paragraph 5, command and signal, to the operation order.
Final draft operation order products.	Participate in staff plans and orders crosswalk, as required.	Final annex H (Signal) to the operation order.
	Provide final input to the risk assessment specific to signal support.	Final appendix 2 (Network Operations) to annex H (Signal).
	Produce operation order products.	Final appendix 3 (Network Diagrams) to annex H (Signal)
	Participate in the operation order briefing and confirmation briefing, as required.	Final appendix 4 (Satellite Communications) to annex H (Signal).
		Final appendix 5 (Foreign Data Exchanges) to annex H (Signal).
		Final appendix 6 (Spectrum Management) to annex H (Signal).
		Final appendix 7 (Information Services) to annex H (Signal).

Paragraph 5 (Command and Signal) of Operation Plans and Orders

B-37. The G-6 (S-6) usually writes paragraph 5 (Command and Signal) of the base plan or order. The G-6 (S-6) lists task-organized units in the appropriate annexes. Figure B-1 on page B-13 shows a sample paragraph 5 for an operation order.

[CLASSIFICATION]

OPERATION PLAN/ORDER [number] [code name]—[issuing headquarters] [(classification of title)]

5. (U) Command and Signal.

a. (U) Command.

(1) (U) Location of Commander and Key Leaders. *State where the commander and key leaders intend to be during the operation, by phase if the operation is phased.*

(2) (U) Succession of Command. *State the succession of command if not covered in the unit's standard operating procedures.*

(3) (U) Liaison Requirements. *State liaison requirements not covered in the unit's standard operating procedures.*

b. (U) Control.

(1) (U) Command Posts. *Describe the employment of command posts, including the location of each command post and its time of opening and closing, as appropriate. State the primary controlling command post for specific tasks or phases of the operation (for example, "The division tactical command post will control the air assault.").*

(2) (U) Reports. *List reports not covered in unit standard operating procedures. Refer to Annex R (Reports) as required.*

c. (U) Signal. *Describe the concept of signal support, including location and movement of key signal nodes and critical electromagnetic spectrum considerations throughout the operation. Refer to Annex H (Signal) as required.*

ACKNOWLEDGE: *Provide instructions for how the addressees acknowledge receipt of the operation plan or operation order. The word 'acknowledge' may suffice. Refer to the message reference number, if necessary. Acknowledgement of an operation plan or operation order means that it has been received and understood.*

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

The commander or authorized representative signs the original copy of the attachment. If the representative signs the original, add the phrase "For the Commander." The signed copy is the historical copy and remains in the headquarters' files.

OFFICIAL:

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

Use only if the commander does not sign the original attachment. If the commander signs the original, no further authentication is required. If the commander does not sign, the signature of the preparing staff officer requires authentication and only the last name and rank of the commander appear in the signature block.

[page number]
[CLASSIFICATION]

Figure B-1. Operation plan or order paragraph 5

Annex H (Signal) to Operation Plans and Orders

B-38. Commanders and staffs use annex H (Signal) to describe how signal supports the concept of operations described in the base plan or order. The G-6 (S-6) develops annex H (Signal) using the five-paragraph attachment format from FM 6-0. (See figure B-2 on pages B-14 through B-17).

[CLASSIFICATION]

Place the classification at the top and bottom of every page of the attachments. Place the classification marking at the front of each paragraph and subparagraph in parentheses. Refer to AR 380-5 for classification and release marking instructions.

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

Include the full heading if attachment is distributed separately from the base order or higher-level attachment.

ANNEX H (SIGNAL) TO OPERATION PLAN/ORDER [number] [code name]—[issuing headquarters] [(classification of title)]

(U) References: *List documents essential to understanding the attachment.*

a. *List maps and charts first. Map entries include series number, country, sheet names or numbers, edition, and scale.*

b. *List other references in subparagraphs labeled as shown.*

c. *Doctrinal references for signal support to operations include FM 6-0, FM 6-02, ATP 6-02.40, ATP 6-02.45, ATP 6-02.53, ATP 6-02.54, ATP 6-02.60, ATP 6-02.70, ATP 6-02.71, ATP 6-02.72, ATP 6-02.73, ATP 6-02.75, and ATP 6-02.90.*

(U) Time Zone Used Throughout the Order: *Write the time zone established in the base plan or order.*

1. (U) Situation. *Include information affecting signal support that paragraph 1 of the operation plan or operation order does not cover, or that needs expansion.*

a. (U) Area of Interest. *Describe the area of interest as it relates to signal support. Refer to Annex B (Intelligence) as required.*

b. (U) Area of Operations. *Describe the area of operations as it relates to signal support. Refer to Appendix 2 (Operation Overlay) to Annex C (Operations).*

(1) (U) Terrain. *Describe the aspects of terrain that impact signal support. Refer to Annex B (Intelligence) as required.*

(2) (U) Weather. *Describe all critical weather aspects that impact signal support, such as rain, flooding, windstorms, and snow, that also may impact network availability or reliability in the area of operations. Refer to Annex B (Intelligence) as required.*

c. (U) Enemy Forces. *List known and templated locations and activities of enemy units for one echelon above and two echelons below. List enemy maneuver and other area capabilities that will impact friendly signal support to operations. State expected enemy courses of action. Refer to Annex B (Intelligence) as required.*

d. (U) Friendly Forces. *Briefly identify the signal mission of friendly forces and the objectives, goals and missions of civilian organizations that impact signal support. Refer to Annex A (Task Organizations) and Annex C (Operations) as required.*

(1) (U) Higher Headquarters' Signal Operations Mission. *Identify and state the signal mission of the higher headquarters.*

(2) (U) Signal Support Operations Impact of Adjacent Units. *Identify and state the missions of adjacent units and other units whose actions have a significant impact on the issuing headquarters' support to operations.*

[page number]
[CLASSIFICATION]

Figure B-2. Operation plan or order annex H (Signal)

[CLASSIFICATION]

ANNEX H (SIGNAL) TO OPERATION PLAN/ORDER [number] [code name]—[issuing headquarters] [(classification of title)]

e. (U) Interagency, Intergovernmental, and Nongovernmental Organizations. *Identify and state the objectives or goals and primary tasks of those non-Department of Defense organizations that may impact the conduct of support to operations or implementation of signal-specific equipment and tactics in the area of operations. Refer to Annex V (Interagency Coordination) as required..*

f. (U) Signal Support to Cyberspace Electromagnetic Activities. *List considerations related to the planning, integration, coordination, and synchronization of Department of Defense information network operations and cyberspace defense with other cyberspace and electronic warfare activities.*

g. (U) Civil Considerations. *Describe the critical aspects of the civil situation that impact voice and data network operations, using the memory aid ASCOPE (areas, structures, capabilities, organizations, people, and events). Refer to Annex B (Intelligence and Annex K (Civil Affairs Operations) as required.*

h. (U) Attachments and Detachments. *List units attached or detached only as necessary to clarify task organization that impacts signal support to operations. Refer to Annex A (Task Organization) as required.*

i. (U) Assumptions. *List key assumptions that pertain to signal support to operations which support development of the annex.*

2. (U) Mission. *State the mission of signal support of the base plan or order.*

3. (U) Execution.

a. (U) Scheme of Signal Support to Operations. *Describe how signal support to operations supports the commander's intent and concept of operations described in the base plan or order. Establish the priorities of support to units for each phase of the operation. Refer to Annex C (Operations) as required.*

(1) (U) Scheme of Defensive Cyberspace Operations. *Describe how defensive cyberspace operations support the commander's intent and concept of operations described in the base plan or order. Outline defensive cyberspace operations that protect against, monitor for, detect (find), analyze (fix), and respond to (finish) cyber threats on the Nonsecure Internet Protocol Router Network, SECRET Internet Protocol Router Network, and Joint Worldwide Intelligence Communications System. Refer to Appendix 1 (Defensive Cyberspace Operations) to Annex H (Signal) as required.*

(2) (U) Scheme of Department of Defense Information Network Operations. *Describe how the commander's intent and concept of operations are supported through actions taken to gain and maintain access to the cyberspace domain through resource allocation, configuration, continuous monitoring of performance and effectiveness, event handling, and security functions that operate and sustain the Non-classified Internet Protocol Router Network, SECRET Internet Protocol Router Network, and Joint Worldwide Intelligence Communications System. Refer to Appendix 2 (Department of Defense information network operations) to Annex H (Signal) as required.*

(3) (U) Scheme of Voice, Video, and Data Routing. *Describe how the routing and movement of voice, video, and data network traffic via primary and alternate routes support the commander's intent and concept of operations described in the base plan or order. Establish the priorities of support to units for each phase of the operation. Provide a detailed network diagram, including the internet protocol scheme of the network being established. Refer to Appendix 3 (Voice, Video, and Data Network Diagrams) to Annex H (Signal) as required.*

[page number]
[CLASSIFICATION]

Figure B-2. Operation plan or order annex H (Signal) (continued)

[CLASSIFICATION]

ANNEX H (SIGNAL) TO OPERATION PLAN/ORDER [number] [code name]—[issuing headquarters] [(classification of title)]

(4) (U) Scheme of Satellite Communications. *Describe how satellite communications support the commander's intent and concept of operations described in the base plan or order. Establish the priorities of support to units for each phase of the operation. Provide a chart for all required frequencies, access times, access dates, and in the case of IP-based satellite communications systems, provide the internet protocol scheme for the modem, as well as the Non-classified Internet Protocol Router Network and SECRET Internet Protocol Router Network routers. (This subparagraph will serve as a reference to units along with attachments). Refer to Appendix 4 (Satellite Communications) to Annex H (Signal) as required.*

(5) (U) Scheme of Foreign Data Exchanges. *Describe how foreign data exchanges support the commander's intent and concept of operations described in the base plan or order. Outline procedures to prevent unauthorized disclosure and release of classified information on the SECRET Internet Protocol Router Network and the Joint Worldwide Intelligence Communications System. Outline the information to be disclosed to, released to, or received from foreign entities and the planned approach, including safeguarding steps to be taken. Refer to Appendix 5 (Foreign Data Exchanges) to Annex H (Signal) as required.*

(6) (U) Spectrum Management Operations. *Describe how spectrum management operations support the commander's intent and concept of operations described in the base plan or order. Outline the effects the commander wants to achieve while prioritizing tasks for spectrum management operations. List objectives and the primary tasks to achieve these objectives. Refer to Appendix 6 (Spectrum Management Operations) to Annex H (Signal) as required.*

(7) (U) Scheme of Information Services. *Describe how information services on Non-classified Internet Protocol Router Network, SECRET Internet Protocol Router Network, and the Joint Worldwide Intelligence Communications System will be provided and integrated to support the commander's intent and concept of operations described in the base plan or order. Explain how information will be staged and the dissemination of that information controlled to facilitate data collection, processing, storage, discovery, and access by the user. Refer to Appendix 7 (Information Services) to Annex H (Signal) as required.*

b. (U) Tasks to Subordinate Units. *List signal support to operations tasks assigned to subordinate signal units not contained in the base order. Each task must include who (the subordinate unit assigned the task), what (the task itself), when, where, and why (purpose). Include tasks for supporting interagency, intergovernmental, and nongovernmental organizations. Use a separate subparagraph for each unit. List units in task organization sequence. Place tasks that affect two or more units in paragraph 3c (Coordinating Instructions).*

c. (U) Coordinating Instructions. *List only instructions applicable to two or more subordinate units not covered in the base plan or order.*

4. (U) Sustainment. *Identify priorities of sustainment for signal support to operations key tasks and specify additional instructions as required in the paragraph below. Refer to Annex F (Sustainment) as required.*

a. (U) Logistics. *Use subparagraphs to identify priorities and specific instructions for signal logistics support. Refer to Annex F (Sustainment) and Annex P (Host-Nation Support) as required.*

[page number]
[CLASSIFICATION]

Figure B-2. Operation plan or order annex H (Signal) (continued)

[CLASSIFICATION]

ANNEX H (SIGNAL) TO OPERATIONS PLAN/ORDER [number] [code name]—[issuing headquarters] [(classification of title)]

b. (U) Personnel. *Use subparagraphs to identify priorities and specific instructions for human resources support, financial management, legal support, and religious support. Refer to Annex F (Sustainment), as required.*

c. (U) Health Service Support. *Identify availability, priorities, and instructions for medical care. Refer to Annex F (Sustainment), as required.*

5. (U) Command and Signal.

a. Command.

(1) (U) Location of the Commander and Key Leaders. *State the location of the commander and key signal unit commanders and staff officers.*

(2) (U) Succession of Command. *State the succession of command, if not covered in the unit's standard operating procedures.*

(3) (U) Liaison Requirements. *State the signal liaison requirements not covered in unit standard operating procedures.*

b. Control.

(1) (U) Command Posts. *Describe the employment of signal command posts, including the location of each command post and its time of opening and closing.*

(2) (U) Reports. *List reports not covered in standard operating procedures. Describe signal reporting requirements for subordinate units. Refer to Annex R (Reports), as required.*

c. (U) Signal. *List signal operating instructions for signal support to operations as needed, as well as primary and alternate means of communications with both military and nonmilitary organizations conducting signal support to operations. Consider operations security requirements.*

(1) (U) *Describe the networks to monitor for reports.*

(2) (U) *Address any support to operations, communications, or digitization connectivity requirements or coordination necessary to meet functional responsibilities (consider telephone listing).*

ACKNOWLEDGE: *Include only if attachment is distributed separately from the base order.*

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

The commander or authorized representative signs the original copy of the attachment. If the representative signs the original, add the phrase "For the Commander." The signed copy is the historical copy and remains in the headquarters' files.

OFFICIAL:

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

Use only if the commander does not sign the original attachment. If the commander signs the original, no further authentication is required. If the commander does not sign, the signature of the preparing staff officer requires authentication and only the last name and rank of the commander appear in the signature block.

[page number
[CLASSIFICATION]

Figure B-2. Operation plan or order annex H (Signal) (continued)

Attachments to Annex H

B-39. Appendixes and their associated tabs provide additional information required to implement the scheme of signal support detailed in annex H. The format and content for appendixes and tabs follow unit standard operating procedures. Appendixes and suggested tabs include—

- Appendix 1—Defensive cyberspace operations.
  - Tab A—Scheme of network protection.
  - Tab B—Defensive cyberspace operations incident battle drill.
  - Tab C—Cybersecurity compliance report.
  - Tab D—Vulnerability and patch reports.
  - Tab E—Defensive cyberspace operations incident report.
- Appendix 2—Department of Defense information network operations.
  - Tab A—Network node allocation and organization.
  - Tab B—Network outage procedures and report.
  - Tab C—Scheme of network monitoring.
  - Tab D—Scheme of COMSEC distribution.
  - Tab E—Scheme of COMSEC compromise procedures.
  - Tab F—COMSEC compromise procedures.
- Appendix 3—Voice, video, and data network diagrams.
  - Tab A—Voice (wide-area network and local area network) logical network diagram.
  - Tab B—Data (wide-area network and local area network) logical network diagram.
  - Tab C—Scheme of tactical radio allocation and employment.
  - Tab D—Voice over Internet protocol phone book.
- Appendix 4—Satellite communications.
  - Tab A—Warfighter Information Network-Tactical satellite transmission diagram.
  - Tab B—Scheme of Tactical Satellite Communications Employment.
- Appendix 5—Foreign data exchanges.
  - Tab A—Coalition forces network diagram.
  - Tab B—Scheme of foreign liaison employment.
- Appendix 6—Spectrum management operations.
  - Tab A—Signal operating instructions (tactical radios).
  - Tab B—Signal operating instructions (Force XXI Battle Command, Brigade and Below; Blue Force Tracking; Joint Capabilities Release; or Joint Battle Command-Platform role name directory).
  - Tab C—VHF and UHF line of sight analysis (single-channel ground and airborne radio system, advanced networking wideband waveform, soldier radio waveform, and highband networking waveform).
  - Tab D—High frequency analysis charts.
- Appendix 7—Information services.
  - Tab A—Scheme of information and knowledge management.
  - Tab B—Scheme of Force XXI Battle Command, Brigade and Below; Blue Force Tracking; Joint Capabilities Release; and Joint Battle Command-Platform allocation and employment.
  - Tab C—Scheme of mission command information system employment (reference annex Q, appendix 3—mission command information system integration matrix).

RAPID DECISION-MAKING AND SYNCHRONIZATION PROCESS

B-40. Operational and mission variables continually change during mission execution. This often invalidates or weakens the chosen course of action. The rapid decision-making and synchronization process allows

commanders and staffs to adjust the operation order to the current situation. When using this technique, the following considerations apply—

- Rapid is often more important than process.
- Much of the process may be mental, rather than written.
- Rapid decision making should be part of the battle drills for current operations integration cells, future operations cells, or both.

B-41. While the military decision-making process seeks the optimal solution, the rapid decision-making and synchronization process seeks a timely and effective solution within the commander's intent, mission, and the concept of operations. Using the rapid decision-making and synchronization process lets leaders avoid the time-consuming requirements of developing decision criteria and comparing courses of action. Under the rapid decision-making and synchronization process, leaders combine their experience and intuition to quickly reach situational understanding. Based on this, they develop and refine workable courses of action.

B-42. The rapid decision-making and synchronization process is based on an existing order and the commander's priorities as expressed in the order. The most important of these control measures are the commander's intent, the concept of operations, and the commander's critical information requirements. The rapid decision-making and synchronization process includes five steps—

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

B-43. The first two steps may be performed in any order or concurrently. The last three are performed iteratively until commanders identify an acceptable course of action. Refer to FM 6-0 for more information about the rapid decision-making and synchronization process.

ADDITIONAL PLANNING CONSIDERATIONS

B-44. The military decision-making process might not address the full scope of planning for signal support. Army forces plan, prepare, execute, and assess signal support in collaboration with joint, interorganizational, and multinational mission partners, as required. Whether signal support is organic to the unit or provided from pooled theater assets, commander involvement and comprehensive situational awareness of cyberspace and the electromagnetic spectrum are critical to mission success.

B-45. Army units need to coordinate or interact with joint forces in the conduct of operations. Commanders and staffs must be familiar with joint planning systems and processes, including the joint planning process and Adaptive Planning and Execution. Refer to JP 5-0 for more information about joint planning.

B-46. The G-6 (S-6) staff assists the protection cell's personnel recovery coordination section when preparing appendix 13 (Personnel Recovery) to annex E (Protection). Refer to FM 3-50 for details about the G-6 (S-6) section's responsibilities in personnel recovery planning.

Note. For more details about the signal staff's role during each step of the military decision-making process, see the S-6 disk resources on the Cyber Lessons and Best Practices Website.

PLANNING CONSIDERATIONS IN A DEGRADED ENVIRONMENT

B-47. Communications planners must understand the commander's concept of operations and intent. Because there might not be sufficient communications capacity for all requirements in a degraded environment, planners need a clear understanding of the overall communications architecture and how it can support the commander's priority effort. The G-6 (S-6) coordinates with other staff sections during the military decision-making process and considers—

- Communications requirements for each warfighting function.
- Capabilities and limitations of available communications systems.

- Requirements for joint, interorganizational, and multinational interoperability.
- Detailed line of sight analysis.
- HF analysis.
- Redundancy in means to communicate—PACE plan.
- Integration of all available signal assets.
- Method of deployment—sequence assets to coincide with the arrival of forces.
- Command post locations.
- The use of retransmission, digital network links, and node placement.
- Satellite communications requirements.
- Priorities of support to manage available communications bandwidth.
- Spectrum requirements for emitters, sensors, radars, and any other assets that rely on a frequency.
- COMSEC distribution plans.
- Initial task organization and expected changes.
- Signal and COMSEC procedures.
- Conduct of communications rehearsals.

TROOP LEADING PROCEDURES

B-48. Troop leading procedures extend the military decision-making process to the small-unit level. The military decision-making process and troop leading procedures are similar but not identical. They are both linked by the basic Army problem-solving process. Commanders with a coordinating staff use the military decision-making process as their primary planning process. Company-level and smaller units lack formal staffs and use troop leading procedures to plan and prepare for operations. This places the responsibility for planning primarily on the commander or small-unit leader (FM 6-0).

B-49. Troop leading procedures are an eight-step process:

- Step 1—receive the mission.
- Step 2—issue a warning order
- Step 3—make a tentative plan.
- Step 4—initiate movement.
- Step 5—conduct reconnaissance.
- Step 6—complete the plan.
- Step 7—issue the order.
- Step 8—supervise and refine.

B-50. The first three steps of troop leading procedures normally occur in order. The order of the remaining steps depends on the tactical situation. Depending on the situation, some steps may require repeating. The final step, supervise and refine, takes place throughout the process.

B-51. The steps of troop leading procedures largely parallel the higher headquarters military decision-making process. A higher headquarters warning order or operation order generally triggers company and below planning using troop leading procedures. Figure B-3 on page B-21 illustrates the parallels between the military decision-making process and troop leading procedures. Refer to FM 6-0 for more detailed information about troop leading procedures.

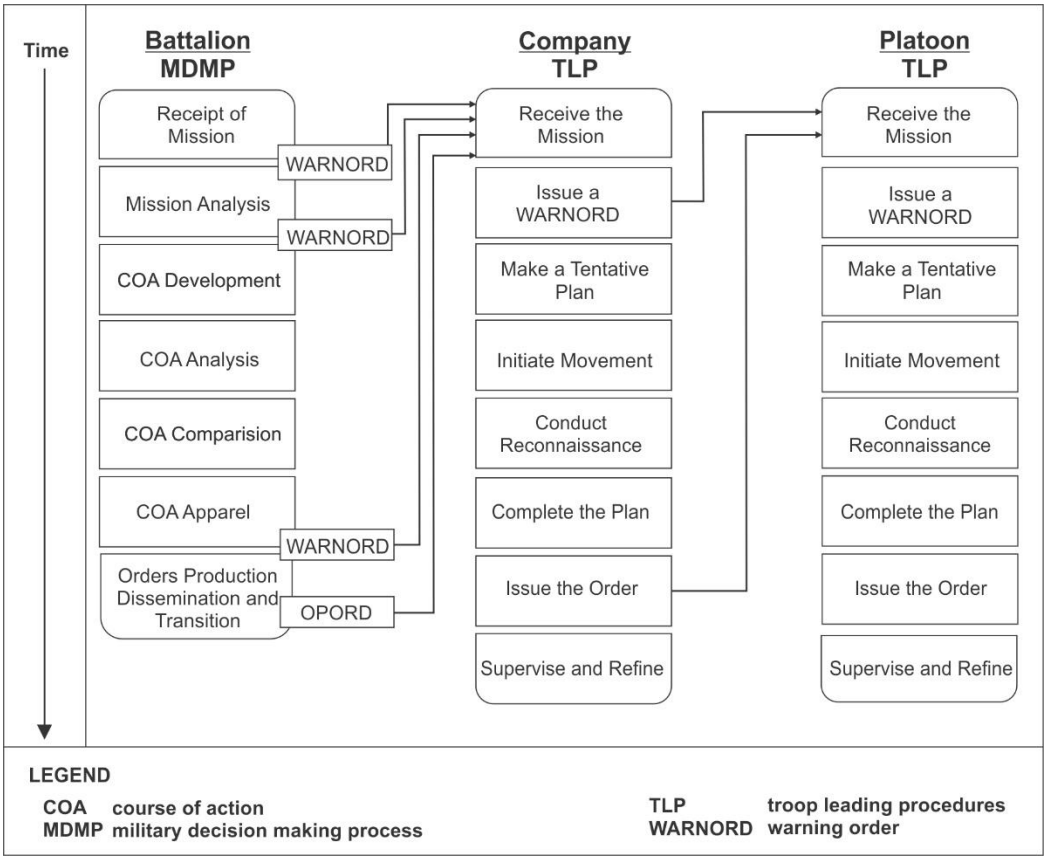


Figure B-3. Parallel sequences of the military decision-making process and troop leading procedures.

SPECTRUM MANAGEMENT

B-52. The spectrum manager uses automated spectrum management tools to assist in electromagnetic spectrum planning and to define support requirements. Planners coordinate frequency use before activating any emitter to mitigate or eliminate electromagnetic interference with friendly systems. The spectrum manager considers—

- Transmitter and receiver locations.
- Antenna technical parameters and characteristics.
- Number of frequencies desired and separation requirements.
- Alternate frequencies for key radio networks.
- Nature of the operation (fixed, mobile land, mobile aeronautical, and over water or maritime).
- Physical effects of the operational environment (ground and soil type, humidity, and topology).
- All spectrum-dependent equipment to be employed, including emitters, sensors, and unmanned aerial sensors.
- Start and end dates for use.
- Restricted and taboo frequencies.

Note. Refer to ATP 6-02.70 for more information about spectrum management.

SIGNAL SITE ANALYSIS AND SELECTION

B-53. The operating characteristics, capabilities, and limitations of various communications systems create specific requirements for acceptable operating locations. Signal sites must be able to accomplish their assigned missions while remaining supportable and defensible.

SITE ANALYSIS

B-54. The G-6 (S-6) should conduct a signal site analysis of the entire area of operations, if possible. Signal site analysis and selection is a collaborative effort between the G-6 (S-6) and the G-3 (S-3). A thorough site analysis enables a meaningful course of action comparison during planning and provides flexibility when executing operations. The G-6 (S-6) analysis focuses on the ability of communications systems to provide coverage from the proposed site. The G-3 (S-3) analysis focuses on mobility, survivability, and sustainability. If the mission changes and operations move to another area, planners should already know which areas they can support with effective communications.

B-55. Signal planners consider the operating characteristics, limitations, and effective planning distance for each available communications asset. As planners define communications requirements, the number of retransmission sites needed to cover the operational area may help determine supportability of proposed courses of action during the military decision-making process.

B-56. The G-6 (S-6) coordinates with the G-2 (S-2) for terrain analysis and the current threat estimate. Signal planners evaluate the terrain (including man-made features) in the operational area to visualize how they can support the mission. Terrain and structures can render some communications systems ineffective. Planners consider the current threat estimate to prevent placing communications sites near known or anticipated enemy positions.

Link Geometry

B-57. The G-6 (S-6) analyzes the terrain to determine how to make the geometry of the operations work in favor of friendly forces. Improper link geometry makes it easier for the enemy to use direction finding jamming capabilities.

B-58. When possible, terrestrial line of sight communications links should parallel the forward line of own troops. This keeps the primary signal strength of U.S. transmissions in friendly terrain. Deploying units and communications systems perpendicular to the forward line of own troops aims transmissions toward the enemy and makes it easier for the enemy to jam communications.

Terrain Masking

B-59. When possible, command post locations should place terrain features and manmade structures between friendly communications systems and enemy positions. This may require moving senior headquarters farther forward and using more jump or tactical command posts to ensure commanders can continue to direct their units effectively.

Antenna Placement

B-60. Command post locations generally determine antenna locations. The proper installation and positioning of antennas around command posts is critical. G-6 (S-6) planners and system operators should position antennas and radio frequency emitters as far as practical from the command post to spread out the electromagnetic signature.

SITE SELECTION

B-61. Based on the signal site analysis, the G-6 (S-6) recommends a signal site for each proposed course of action during the military decision-making process. The final site selected must be—

- Able to support the selected course of action.
- Logistically supportable.

- Defensible—
  - Defensive plan
  - Escape routes.
  - Cover.
  - Concealment.

B-62. Operating against a peer threat may require locating the signal site away from the supported command post. This way, if an enemy locates and destroys communications systems, they do not destroy the entire command post capability. Operating signal systems away from the supported command post creates additional physical security and site defense requirements.

RECONNAISSANCE

B-63. Before occupying a signal site, leaders should reconnoiter the designated area. The site reconnaissance might find unanticipated conditions that make the selected site unacceptable. This would require adjusting the operation plan or order to select a new signal site. The reconnaissance team should consist of the company leader, the transmission supervisor (if applicable), node supervisor (if applicable), and a security team. The makeup of the reconnaissance team depends on the type of unit. The reconnaissance team maintains single-channel radio communications with their parent headquarters. The reconnaissance team should—

- Ensure the selected site can support the unit's communications requirements.
- Ensure the site is large enough to accommodate and tactically disperse all communications assemblages on the site.
- Determine whether the selected site is securable and defensible. The reconnaissance team considers—
  - The size of the site.
  - The number of personnel available to defend the site.
  - Entrances and avenues of approach.
  - Concealment from major roads or other vantage points. This may involve traveling around the entire site from a distance to visualize what the enemy would see.
- Verify the site is close enough to the supported unit command post to connect with the signal systems. Increasing distance between signal assemblages and subscribers complicates troubleshooting.
- Verify line of sight between stations for multichannel radio links. Line of sight planning range is about 40 kilometers, or 28 miles.
- Ensure terrain and man-made structures will not interfere with communications equipment and links.

SIGNAL SITE SECURITY AND DEFENSE

B-64. Site defense plans depend on the size and type of signal site and whether it is colocated with the supported unit. Planners coordinate with the G-2 (S-2) staff for the current threat estimate and the G-3 (S-3) staff for security force requirements when planning site defense.

Colocated Sites

B-65. Usually, these are larger signal elements, up to platoon size, supporting a unit command post. The signal personnel assist in perimeter defense. The supported unit headquarters conducts the overall defense of the command post. The signal element coordinates closely with the supported unit.

Remote Sites

B-66. Planners must coordinate for security and sustainment services when deploying signal sites remotely from the supported unit. When a signal site does not colocate with the supported headquarters, the signal element conducts site defense. They must also be prepared to survive enemy air, artillery, and chemical, biological, radiological, and nuclear attack with little outside assistance. Because of their size and limited

defensive capabilities, signal elements need assistance from the supported unit to defend against a large-scale assault.

Node Sites

B-67. Platoon-sized signal elements may or may not colocate with the command post or other elements of the supported unit. Based on the threat level, the signal site commander plans site defense and coordinates with nearby units for mutual support.

Small Teams

B-68. Small teams often operate from isolated positions, usually for retransmission or wireless network extension. Teams should try to remain concealed and report enemy activity to higher headquarters. The teams conduct risk assessments at remote sites to determine the likelihood of mission success. Supported unit leaders must carefully track threats and move teams quickly when in danger.

Appendix C

Visual Information

Visual information and COMCAM provide vital information to support decision making. Because the available support is limited, the operational chain of command validates and approves support requests before committing COMCAM assets. Archived visual information products are available from a centralized repository.

PROCEDURES FOR REQUESTING COMBAT CAMERA SUPPORT

C-1. Planners develop COMCAM requirements and submit them to Joint Chiefs of Staff through the combatant command personnel directorate and operations directorate (J-3) by entering the requirement into the Joint Capabilities Requirements Manager. The chain of command validates and resources rotational and contingency COMCAM requirements supporting joint operations through the global force management process. When the supporting Service sources the requirement, they enter the personnel and logistics information into the Joint Operation Planning and Execution System for assignment of unit line numbers.

C-2. Any Service's COMCAM unit or activity can fulfill a COMCAM requirement. COMCAM assets belong to their parent Service until placed under the operational or tactical control of a supported unit.

C-3. Before sending a tasking message, the requesting unit should contact the COMCAM unit to discuss the type of support and timeframe required. This coordination should take place as early as possible. The COMCAM unit evaluates the feasibility and supportability of the requirement. If the COMCAM unit cannot support the requirement, the unit helps identify other support resources. Figure C-1 on page C-2 shows the format for an official COMCAM support request.

Note. Verbal contact is not a commitment or an agreement to provide support.

```
UNIT NAME: 55TH SIGNAL COMPANY
UIC: WDBCAA
LOCATION: FT. MEADE, MARYLAND 20755
PHONE: (301) 677-5343 DSN 923

TO:
USACOM NORFOLK VA//J36//
DA WASHINGTON DC//DAMO-ODO//

INFO:
HQDA WASHINGTON DC//SAIS-PAC-V//
AMFINFOS WASHINGTON DV//DVI//
CDRFORSCOM FT BRAGG NC//G3//NETCOM FT HUACHUCA AZ//G3//
7TH SIG CMD (THEATER) FT GORDON//NETC-SFC-OPY (G3)//
21ST SIG BDE FT DETRICK MD//S3//
CDR 114TH SIG BN FT DETRICK MD//CC/NETC-SYR// (USE FOR UNCLASSIFIED MESSAGES)
CDR 114TH SIG BN FT DETRIC MD//CC/NETC-SYR// (USE FOR CLASSIFIED MESSAGES)
CDR 55TH SIGNAL CO FT MEADE MD//CC/NETC-SYR-F//

4.B. (U/FOUO) UNIT CAPABILITY REQUESTED:
UNIT TYPE CODE:
4.B.1. (U/FOUO) DESTINATION:
4.B.2. (U/FOUO) DEPLOYMENT DATES:
4.B.3. (U/FOUO) DEPLOYMENT DURATION:
4.B.4. (U/FOUO) MISSION JUSTIFICATION:
4.B.4.A. (U/FOUO) TASK:
4.B.4.B. (U/FOUO) PURPOSE:
4.B.4.C. (U/FOUO) COMMAND AND CONTROL:
4.B.4.D. (U/FOUO) REPORTING INSTRUCTIONS:
```

Figure C-1. Combat camera support request format

PROCEDURES FOR REQUESTING VISUAL INFORMATION PRODUCTS

C-4. Units prepare requests for visual information products on official letterhead signed by a branch or unit head. They may submit requests to the Defense Imagery Management Operations Center by facsimile, postal mail, or e-mail.

C-5. The following information is required when requesting imagery—

- Subject and/or image identification number.
- Unit, location, event, or operation name.
- Date or date range.
- Equipment or equipment type to represent, if any.
- Action requester wants to see.
- Media format, size, and quantity.
- Date needed.
- Requester’s name, rank, and position title.
- Requester’s Defense Switched Network and commercial telephone numbers.
- Complete official mailing address, including building and room or suite number.
- How media is to be used (briefing, training).
- For motion media requests, the approximate total number of minutes needed for each subject.

C-6. The Defense Imagery Management Operations Center provides high-resolution photograph archive files for download through the defense imagery Website. Requesters bear expenses for hard copy production and duplication. Official government customers can also obtain visual information products from the Defense Imagery Website.

This page intentionally left blank.

Appendix D

Signal Systems Maintenance

This appendix outlines two-level maintenance at brigade and below. It discusses communications-electronics maintenance and the logistics support provided to build and preserve operational readiness. Early detection by the operator, crew, or maintainer, correction of failures as far forward as possible, and prompt replenishment of repair parts are essential to readiness.

MAINTENANCE MANAGEMENT

D-1. Army organizations are required to establish standard operating procedures and maintenance management processes to sustain, repair, evacuate, and report maintenance 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.

TWO-LEVEL MAINTENANCE

D-2. The Army utilizes a tiered, two-level maintenance system comprised of field and sustainment maintenance. Command teams, maintenance personnel, and planners must have a complete understanding of two-level maintenance fundamentals to plan and execute their mission. See table D-1 for the alignment of units to the type of maintenance performed.

- **Field maintenance** takes place as close to the point of use as possible. The owning unit retains the equipment or receives it back from the maintenance support facility. Equipment operators, operator-maintainers, and ordnance-trained maintainers perform field maintenance. Army maintenance units also provide field maintenance support.
- **Sustainment maintenance** restores equipment to a national standard, after which the equipment is returned into the supply system. Sustainment maintenance requires evacuating the equipment to a support facility. When a unit sends equipment to a sustainment maintenance organization, the owning unit usually removes the equipment from its property book. Only in rare instances, such as unit reset, does the equipment return to the owning unit.

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

Field Maintenance	***Sustainment Maintenance***
Operator/crew	Army field support brigade (management)
Forward support company	Army field support battalion
Field maintenance company	United States Army Materiel Command support formations
Support maintenance company	Army depots
Other units with assigned Ordnance School-trained maintainers	Logistics readiness center (installation)

D-3. The goal of the maintenance system is to reduce repair times by repairing or replacing components, modules, and assemblies as far forward as possible by maximizing reliance on rapid repair parts distribution.

FIELD MAINTENANCE

D-4. Field maintenance consists of two subcategories, operator or crew and Ordnance Corps trained maintainer. Field maintenance restores unserviceable equipment, communications systems, or weapon systems using line replaceable units or modules and component replacement or repair. The owning unit normally performs field maintenance using organic tools and test equipment. The unit should retain and repair the item until it is ready to return to service. Field maintenance is not limited to simply remove and replace actions. If the operator, crew, or maintainer have the skills, special tools, repair parts, references, and adequate time to repair an item, the unit should not evacuate equipment for sustainment maintenance.

D-5. The brigade support battalion has low-density specialty maintainers to maintain specialized equipment in the brigade combat team. These personnel perform maintenance the forward support companies are not structured to accomplish including missiles, fire control systems, and signal systems.

D-6. Field maintenance includes actions performed by crew members, operators, and maintenance personnel, such as—

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

D-7. Field maintenance is always repair and return to the user. Maintenance personnel at echelons below brigade level reside in the owning unit, forward support company, and field maintenance company.

Operator and Crew Maintenance

D-8. Operators and crews perform field maintenance on their assigned equipment as outlined in the equipment operator's manual. The operator or crew is typically the first to observe a fault or failure. In many instances, operators or crews can repair the fault or minimize its impact, enabling mission completion. Operators and crews may also initiate maintenance tasks in response to fault or failure indicators or instrumentation. Typical tasks consist of inspecting, servicing, lubricating, adjusting, and replacing minor components or assemblies, as authorized in the maintenance allocation chart. Operator and crew tasks in a maintenance allocation chart refer to the applicable technical manual and use basic issue items and onboard spares.

D-9. Operators and crews are specialists on their systems. They receive formal military occupational specialty or functional training on diagnosing system faults. Operators and crews troubleshoot their systems using the operator's manual and simplified or embedded diagnostic equipment to identify, isolate, and trace problems. Operators and crews include signal or military intelligence military occupational specialties, or a maneuver unit's master gunner, who receive advanced individual training, specialized courses, and in some instances, specialized tools. Their primary focus is the system's performance and integrity. After operators and crews exhaust their maintenance capabilities, they rely on maintenance personnel to conduct field maintenance on their equipment. Most maneuver units receive this maintenance support from the forward support company.

Maintainer Maintenance

D-10. Maintainer maintenance is performed by Ordnance School-trained maintenance personnel. 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 by a trained maintainer.

D-11. Depending on the system and military occupational specialty involved, the definition of a line replaceable unit or shop replaceable unit is flexible. The characterization of line or shop replaceable units for wheeled and tracked vehicles, radar, or communications systems shifts as the field maintenance

troubleshooting increases in complexity. Operator-maintainers working with communications systems and communications-electronics equipment, armament routinely perform tasks other maintainers would consider sustainment-level maintenance.

SUSTAINMENT MAINTENANCE

D-12. Since it is closer to the point of use, field maintenance is the preferred method of repair. However, operators, crews, and unit maintenance personnel sometimes lack the skills, special tools, repair parts, or references to complete repairs. This may require evacuating equipment for sustainment maintenance. Based on the extent of damage or failure, leaders use their professional judgment to determine the best course of action, based on operational and mission variables.

D-13. The intent of sustainment maintenance is to perform commodity-oriented repairs to return items to a national standard, providing a consistent and measurable level of reliability. Sustainment maintenance supports both operational forces and the Army supply system. Sustainment maintenance is comprised of two subcategories—below depot-level sustainment maintenance and depot-level sustainment maintenance.

Depot Maintenance

D-14. Tobyhanna Army Depot provides depot-level sustainment maintenance for communications-electronics systems, including joint satellite communications and joint command, control, communications, computers, intelligence, surveillance, and reconnaissance systems. Besides depot repairs and spares management, Tobyhanna Army Depot can provide on-site depot-level technical assistance.

D-15. Tobyhanna's forward repair activities provide depot-level sustainment presence at locations inside and outside the continental United States. Tobyhanna field service representatives provide depot-level technical assistance visits for on-site troubleshooting, repair, and configuration assistance worldwide.

Below Depot Maintenance

D-16. The United States Army Communications-Electronics Command Field Sustainment Support Division has seven regional support centers aligned with the Army field support brigades. Regional support centers provide forward logistical support, including care of supplies in storage, warehousing, below depot sustainment maintenance, and return maintenance authorizations for warranty items. The regional support centers can react rapidly to warfighter requirements and support surge requirements, if necessary. Regional support centers mainly support commercial off-the-shelf and non-standard equipment.

D-17. United States Army Communications-Electronics Command provides below depot sustainment maintenance for United States Army Training and Doctrine Command training base tactical equipment at Fort Huachuca, Arizona and Fort Gordon, Georgia. This includes associated support items of equipment for the systems.

D-18. United States Army Communications-Electronics Command's logistics assistance representatives provide commanders the technical guidance necessary to resolve problems with weapon systems, equipment, and logistics. Logistics assistance representatives help solve readiness issues at unit level, and assist with logistics problems beyond the unit's resources or capabilities to resolve through—

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

COMMUNICATIONS-ELECTRONICS MAINTENANCE

D-19. The unique maintenance requirements of signal equipment and the need to maintain the DODIN-A with minimal downtime requires more responsive maintenance procedures. Some signal military occupational specialties are operator-maintainers who 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 viability of the network.

NETWORK SYSTEMS MAINTENANCE

D-20. Maintaining the DODIN-A requires continual coordination between signal leaders and staffs. The G-6 (S-6) and the division and brigade signal leaders work across organizational boundaries to sustain their portions of the DODIN-A.

Communications-Electronics Maintenance in the Maneuver Battalion

D-21. The S-6 works in conjunction with the logistics staff, support operations, communications-electronics maintenance shop, and the forward support company commander to develop a comprehensive maintenance plan. The maintenance plan includes coordination for contractor field service representative support. The maintenance plan becomes part of the unit's maintenance standard operating procedure. This ensures there are clearly understood procedures to preserve the battalion's maintenance readiness. The signal support systems specialist in the brigade and battalion S-6—

- Replaces defective line replaceable units or modules in communications-electronics systems, COMSEC devices, remote control systems, intercoms, and automated information systems.
- Replaces line replaceable units or modules or evacuates equipment to the forward support company for repair or replacement of faulty communications-electronics equipment and automated information systems.
- Repairs and installs the unit's communications-electronics systems wiring and cabling.
- Installs and removes vehicular and base station communications systems, and automated information systems. This includes installation kits, antennas, and cables on all platforms.
- Performs communications-electronics systems testing.
- Maintains test, measurement, and diagnostic equipment calibration records.
- Manages and maintains battery inventory and charging systems.
- Orders and maintains bench stock.
- Applies modifications and directions, such as technical bulletin guidance.

D-22. Maneuver battalions typically receive field maintenance support from the brigade support battalion's forward support company. The forward support company has a maintenance platoon to repair 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 has a service and recovery section to perform battle damage assessment and repair.

D-23. 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 maneuver battalion's logistics staff.

Communications-Electronics Maintenance in the Brigade

D-24. 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 maintain operations.

D-25. Each maneuver brigade has an assigned brigade support battalion with a forward support company and a field maintenance company. In the other brigades, the forward support company supports the maneuver battalions. The field maintenance company supports the brigade headquarters and other non-maneuver units in the brigade.

D-26. The field maintenance company has a base support platoon to provide electronics equipment maintenance support and conduct float management of communications-electronics equipment to a forward support company. The forward support company focuses on line replaceable units using combat spares from shop stock. The forward support company has a service and recovery section to perform 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

D-27. 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 commander, executive officer, and electronic systems maintenance warrant officer to ensure critical network maintenance, services, repair parts, and spares are available to preserve operational readiness.

Brigade Signal Company

D-28. The brigade signal company coordinates network performance and maintenance issues with the brigade S-6. The brigade signal company has operator-maintainers who perform field maintenance on organic signal equipment. The signal company executive officer coordinates maintenance support for organic equipment and maintains logistical and maintenance oversight for the company.

UNITS WITH NO ORGANIC MAINTENANCE CAPABILITIES

D-29. Some units in the brigade have limited or no organic field maintenance capability or capacity. These units normally receive field maintenance support or augmentation from a supporting maintenance organization. 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 for any equipment or commodity area 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.

This page intentionally left blank.

Appendix E

Requests for Signal Support

Units with no organic signal assets, or units tasked to perform a mission beyond their organic signal capabilities, request signal support through the request for forces process. The signal requirements may be fulfilled in-theater using regionally-aligned forces, or may require resources from the global force pool.

IDENTIFYING SIGNAL REQUIREMENTS

E-1. Units that require signal augmentation do not request a unit, such as an expeditionary signal company, or a communications assemblage, but the operational capability required to accomplish their mission. The requesting unit G-6 (S-6) identifies the signal requirements. Accurately defining requirements simplifies the process of validation as the request routes through successive levels of the chain of command. The G-6 (S-6) determines—

- Services required by type and quantity—
  - NIPRNET.
  - SIPRNET.
  - Joint Worldwide Intelligence Communications System.
  - Secure and nonsecure voice.
  - Video teleconferencing.
  - Coalition—mission partner environment.
  - Commercial services.
- Mission and purpose for each service.
- Period of services—
  - Starting date-time group.
  - Ending date-time group, if known.
- Location of services.

REQUEST FOR FORCES

E-2. Once the G-6 (S-6) identifies the signal requirements, the G-3 (S-3) initiates a request for forces and forwards it to their higher headquarters for validation. For the request for forces to be validated, it must make operational sense. The request for forces identifies—

- The unit requesting support.
- The capability required. Requestors describe the capability clearly enough to identify in lieu of sourcing, if applicable.
- Time needed.
  - Earliest arrival date.
  - Latest arrival date.
- Deployment duration, and whether or not service rotations are authorized.
- Mission justification.
  - Why the capability is required.
  - Operational risk, if not sourced.
  - Mitigation measures available to reduce that risk.

- Similar capabilities in the area of responsibility.
  - Number.
  - Justification why they cannot be used.
- Identify whether the request is for additional or replacement forces.
  - Detailed justification.
  - If additional, what change in the operational environment created the requirement?
- Special training requirements.
- Command and control relationships.
- Urgency.
  - Non-urgent—120 days prior to earliest arrival date.
  - Urgent or emergent—within 120 days.
  - Immediate—within 30 days.

REQUIREMENT VALIDATION

E-3. As the request for forces routes through the chain of command to the geographic combatant commander, each successive level reviews the request to determine—

- Whether the requirements are valid.
- Whether the requested forces are operationally necessary.
- Whether the requirement can be satisfied internally with organic or attached signal elements.
- A sourcing recommendation to fulfill the requirement.

SOURCING

E-4. If the theater army or geographic combatant command can fulfill the requirement with forces already in theater, the geographic combatant command sources the capability internally. The tasking order defines operational, tactical, and administrative control relationships for the supporting and supported units.

E-5. If the geographic combatant cannot fulfill the requirement, the combatant command J-3 forwards the request to the Joint Staff J-3 force management office. The J-3 force management office—

- Validates the unit request.
- Assigns a force tracking number.
- Forwards the request to United States Army Forces command for sourcing.

E-6. United States Army Forces Command G-3—

- Identifies a unit to fulfill the requirement.
- Forwards to the Joint Staff J-3 force management office for allocation.

E-7. The Joint Staff J-3 force management office—

- Approves the source.
- Allocates the requirement in the Joint Capabilities Requirements Manager system.
- Forwards the allocated requirement to U.S. Army Forces Command.

E-8. United States Army Forces Command issues a deployment order to the identified unit. The deployment order identifies the operational, tactical, and administrative control relationships for the supporting and supported units. Figure E-1 on page E-3 outlines the request for forces process.

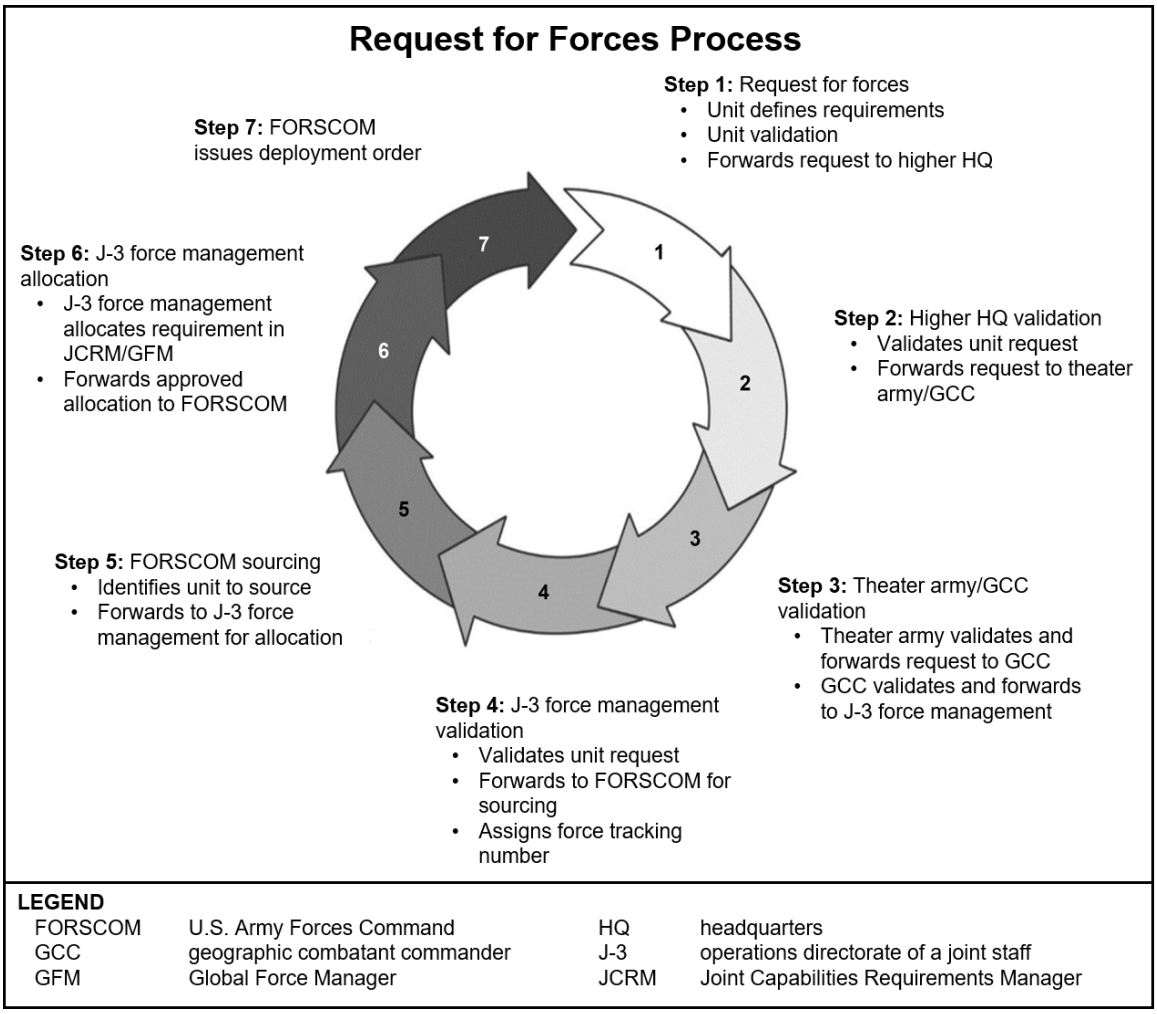


Figure E-1. Request for forces process

This page intentionally left blank.

Source Notes

This division lists sources by page number. Where material appears in a paragraph, it lists both the page number followed by the paragraph number.

1-2. “There is no better example…”: General Martin E. Dempsey, former Chairman of the Joint Chiefs of Staff, Joint Information Environment White Paper, 22 January 2013.

2-40. “A strong case can be made…”: *A History of U.S. Communications Security (U): The David G. Boak Lectures, Vol. II*, National Security Agency, July 1981.

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 FM 6-02 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

ARCYBER	United States Army Cyber Command
CEMA	cyberspace electromagnetic activities
CIO	chief information officer
COMCAM	combat camera
COMSEC	communications security
DISN	Defense Information Systems Network
DODIN	Department of Defense information network
DODIN-A	Department of Defense information network-Army
EW	electronic warfare
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
G-6	assistant chief of staff, signal
HF	high frequency
J-3	operations directorate of a joint staff
J-6	communications system directorate of a joint staff
JTF	joint task force
NETCOM	United States Army Network Enterprise Technology Command
NIPRNET	Non-classified Internet Protocol Router Network
PACE	primary, alternate, contingency, and emergency
S-2	battalion or brigade intelligence staff officer
S-3	battalion or brigade operations staff officer
S-6	battalion or brigade signal staff officer
SC(T)	signal command (theater)
SIPRNET	SECRET Internet Protocol Router Network
VHF	very high frequency

SECTION II – TERMS

adversary

A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged. (JP 3-0)

combat camera

Specially-trained expeditionary forces from Service-designated units capable of providing high-quality directed visual information during military operations. Also called **COMCAM**. (JP 3-61)

command and control

The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of a mission. (JP 1)

command and control system

The arrangement of personnel, processes and procedures, networks, and command posts that enable commanders to conduct operations. (ADP 6-0)

command and control warfighting function

The related tasks and a system that enable commanders to synchronize and converge all elements of combat power. (ADP 6-0)

communications security

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

cybersecurity

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

cyberspace

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

cyberspace electromagnetic activities

The process of planning, integrating, and synchronizing cyberspace and electronic warfare operations in support of unified land operations. Also called **CEMA**. (ADP 3-0)

cyberspace operations

The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. (JP 3-0)

defense-in-depth

An information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. (CNSSI 4009)

defensive cyberspace operations

Missions to preserve the ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity. (JP 3-12)

defensive cyberspace operations-internal defensive measures

Operations in which authorized defense actions occur within the defended portion of cyberspace. (JP 3-12)

defensive cyberspace operations-response actions

Operations that are part of a defensive cyberspace operations mission that are taken external to the defended network or portion of cyberspace without the permission of the owner of the affected system. (JP 3-12)

Department of Defense information network

The set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, 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)

electromagnetic jamming

The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing an enemy's effective use of the electromagnetic spectrum, and with the intent of degrading or neutralizing the enemy's combat capability. (JP 3-13.1)

electromagnetic spectrum

The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. (JP 3-13.1)

electronic warfare

Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called **EW**. (JP 3-13.1)

emission control

The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors; b. mutual interference among friendly systems; and/or c. enemy interference with the ability to execute a military deception plan. (JP 3-13.1)

enclave

A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter. (CNSSI 4009)

enemy

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

field maintenance

On-system maintenance, repair and return to the user including maintenance actions performed by operators .(FM 4-30)

force projection

The ability to project the military instrument of national power from the United States or another theater, in response to requirements for military operations. (JP 3-0)

forcible entry

Seizing and holding of a military lodgment in the face of armed opposition or forcing access into a denied area to allow movement and maneuver to accomplish the mission. (JP 3-18)

hybrid threat

The diverse and dynamic combination of regular forces, irregular forces, terrorists, or criminal elements unified to achieve mutually benefitting effects. (ADP 3-0)

information environment

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

information management

The science of using procedures and information systems to collect, process, store, display, disseminate, and protect data, information, and knowledge products. (ADP 6-0)

information operations

The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. (JP 3-13)

insider threat

A person with placement and access who intentionally causes loss or degradation of resources or capabilities or compromises the ability of an organization to accomplish its mission through espionage, providing support to international terrorism, or the unauthorized release or disclosure of information about the plans and intentions of United States military forces. (AR 381-12)

intelligence preparation of the battlefield

The systematic process of analyzing the mission variables of enemy, terrain, weather, and civil considerations in an area of interest to determine their effect on operations. (ATP 2-01.3)

knowledge management

The process of enabling knowledge flow to enhance shared understanding, learning, and decision making. (ADP 6-0)

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)

military decision-making process

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

military engagement

The routine contact and interaction between individuals or elements of the United States Armed Forces and those of another nation’s armed forces or civilian authorities to build trust and confidence, share information, coordinate mutual activities and maintain influence. (JP 3-0)

mission command

The Army’s approach to command and control that empowers subordinate decision making and decentralized execution appropriate to the situation.. (ADP 6-0)

network enterprise center

The facility that provides and acquires telecommunications and information management services on Army installations. (ATP 6-02.71)

*** network transport**

The processes, equipment, and transmission media that provide connectivity and move data between networking devices and facilities.

offensive cyberspace operations

Cyberspace operations intended to project power by the application of force in or through cyberspace. (JP 3-12)

operational environment

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

operational reach

The distance and duration across which a force can successfully employ military capabilities. (JP 3-0)

retrograde

A defensive task that involves organized movement away from the enemy. (ADP 3-90)

running estimate

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

*** spectrum management operations**

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

spillage

A security incident that results in the transfer of classified information onto an information system not authorized to store or process that information. (CNSSI 4009)

synchronization

The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. (JP 2-0)

technical channels

The chain of authority for ensuring the execution of clearly delineated technical tasks, functions, and capabilities to meet the dynamic requirements of Department of Defense information network operations. (ATP 6-02.71)

threat

Any combination of actors, entities, or forces that have the capability and into to harm United States forces, United States national interests, or the homeland. (ADP 3-0)

unified land operations

The simultaneous execution of offense, defense, stability, and defense support of civil authorities across multiple domains to shape operational environments, prevent conflict, prevail in large-scale ground combat, and consolidate gains as part of unified action. (ADP 3-0)

visual information

Various visual media with or without sound that generally includes still and motion photography, audio video recording, graphic arts, and visual presentations. (JP 3-61)

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)

This page intentionally left blank.

References

All URLs accessed on 26 August 2019.

REQUIRED PUBLICATIONS

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

DOD Dictionary of Military and Associated Terms. July 2019.

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

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS

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

DODD 8140.01. *Cybersecurity Workforce Management.* 11 August 2015.

DODI 5040.02. *Visual Information*. 27 October 2011.

DODI 8500.01. *Cybersecurity*. 14 March 2014.

DODI 8510.01. *Risk Management Framework (RMF) for DOD Information Technology (IT).* 12 March 2014.

JP 1. *Joint Doctrine for the Armed Forces of the United States*. 25 March 2013.

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

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

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 3-18. *Joint Forcible Entry Operations*. 11 May 2017.

JP 3-27. *Homeland Defense*. 10 April 2018.

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

JP 3-61. *Public Affairs*. 17 November 2015.

JP 5-0. *Joint Planning*. 16 June 2017.

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

JP 6-01. *Joint Electromagnetic Spectrum Management Operations*. 20 March 2012.

ARMY PUBLICATIONS

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

ADP 1. *The Army*. 31 July 2019.

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

ADP 3-28. *Defense Support of Civil Authorities*. 31 July 2019.

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

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

ADP 6-0. *Mission Command: Command and Control of Army Forces*. 31 July 2019.

ADP 7-0. *Training.* 31 July 2019.

AR 5-22. *The Army Force Modernization Proponent System*. 28 October 2015.
AR 25-6. *Military Auxiliary Radio System and Amateur Radio Program*. 3 January 2014.
AR 381-12. *Threat Awareness and Reporting Program*. 1 June 2016.
ATP 2-01.3. *Intelligence Preparation of the Battlefield*. 1 March 2019.
ATP 3-05.60. *Special Operations Communications System*. 30 November 2015.
ATP 3-12.3. *Electronic Warfare Techniques*. 16 July 2019.
ATP 3-37.10. *Base Camps*. 27 January 2017.
ATP 3-93. *Theater Army Operations*. 26 November 2014.
ATP 3-94.1. *Digital Liaison Detachment*. 28 December 2017.
ATP 3-96.1. *Security Force Assistance Brigade*. 2 May 2018.
ATP 4-15. *Army Watercraft Operations*. 3 April 2015.
ATP 4-33. *Maintenance Operations*. 9 July 2019.
ATP 5-19. *Risk Management*. 14 April 2014.
ATP 6-0.5, *Command Post Organization and Operations*. 1 March 2017.
ATP 6-01.1. *Techniques for Effective Knowledge Management*. 6 March 2015.
ATP 6-02.40. *Techniques for Visual Information Operations*. 14 January 2019.
ATP 6-02.53. *Techniques for Tactical Radio Operations*. 7 January 2016.
ATP 6-02.54. *Techniques for Satellite Communications*. 5 June 2017.
ATP 6-02.60. *Tactical Networking Techniques for Corps and Below*. 9 August 2019.
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.
ATP 6-02.75. *Techniques for Communications Security Operations*. 17 August 2015.
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 3-22. *Army Support to Security Cooperation*. 22 January 2013.
FM 3-50. *Army Personnel Recovery*. 2 September 2014.
FM 3-53. *Military Information Support Operations*. 4 January 2013.
FM 3-94. *Theater Army, Corps, and Division Operations*. 21 April 2014.
FM 3-96. *Brigade Combat Team*. 8 October 2015.
FM 4-30. *Ordnance Operations*. 1 April 2014.
FM 6-0. *Commander and Staff Organization and Operations*. 5 May 2014.
FM 6-27. *The Commander's Handbook on the Law of Land Warfare*. 7 August 2019.
TB 380-40. *Security: Army Controlling Authority and Command Authority Procedures*. 10 September 2012.
TC 7-100. *Hybrid Threat*. 26 November 2010.
TC 7-100.2. *Opposing Force Tactics*. 9 December 2011.

OTHER PUBLICATIONS

A History of U.S. Communications Security (U): The David G. Boak Lectures, Vol. II. National Security Agency, July 1981. https://www.nsa.gov/news-features/declassified-documents/cryptologic-histories/assets/files/history_comsec_ii.pdf.
American National Standard T1.523.2011. *Alliance for Telecommunications Industry Solutions Telecom Glossary 2011*. 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. (Requires DOD-approved certificate login).

Chairman of the Joint Chiefs of Staff. *Joint Information Environment White Paper*. 22 January 2013. https://www.jcs.mil/Portals/36/Documents/Publications/environmentalwhitepaper.pdf.

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

Defense Information Service Agency. *Enabling the Joint Information Environment: Shaping the Enterprise for the Conflicts of Tomorrow*. 5 May 2014. https://www.disa.mil/~/media/Files/DISA/About/JIE101_000.pdf.

Memorandum, DOD CIO. 15 December 2014. Subject: Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services. https://dodcio.defense.gov/Portals/0/Documents/Cloud/DoD%20CIO%20-%20Updated%20Guidance%20-%20Acquisition%20and%20Use%20of%20Commercial%20Cloud%20Serviices_20141215.pdf.

UNITED STATES LAW

Most acts and public laws are available at https://uscode.house.gov/.

Clinger-Cohen Act

Title 10, United States Code. Armed Forces.

Title 32, United States Code. National Guard.

RECOMMENDED READINGS

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

ADP 4-0. *Sustainment*. 31 July 2019.

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

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

CJCSI 3205.01D. *Joint Combat Camera (COMCAM)*. 20 October 2014.

CJCSM 6510.01B. *Cyber Incident Handling Program*. 10 July 2012.

DODI 8530.01. *Cybersecurity Activities Support to DOD Information Network Operations*. 7 March 2016.

TB 380-41. *Security: Procedures for Safeguarding Accounting and Supply Control of COMSEC Material*. 15 August 2013.

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate Website: https://armypubs.army.mil.

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

WEBSITES

Approved Products List Integrated Tracking System Website (Requires DOD-approved certificate login) https://aplits.disa.mil.

Command, Control, Communications, Computers and Information Management Services List Website (Requires DOD-approved certificate login) https://www.itmetrics.hua.army.mil. (Choose e-mail certificate.)

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

Defense Imagery Website https://www.dimoc.mil.

Index

Entries are by paragraph number.

FM 6-02
13 September 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
1925303

DISTRIBUTION:
Distributed in electronic media only (EMO).

This page intentionally left blank.

PIN: 103938-000