FM 6-02

SIGNAL SUPPORT TO OPERATIONS

JANUARY 2014

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

HEADQUARTERS, DEPARTMENT OF THE ARMY

Field Manual
No. 6-02

Headquarters
Department of the Army
Washington, DC, 22 January 2014

SIGNAL SUPPORT TO OPERATIONS

Contents

Page

Distribution Restriction: Approved for public release, distribution is unlimited.

Figures

Preface

FM 6-02 describes the Signal Regiment support to the Army's mission, commanders, staff officers and signal personnel. This manual establishes the Signal Regiment's roles and responsibilities of organic and non-organic signal forces providing LandWarNet that enable and support the Army's mission at all echelons. It supports the Army's view of how it conducts prompt and sustained operations and sets the foundation for developing the Army techniques publications, which provide techniques information.

The principal audience for FM 6-02 is Army commanders, leaders and staffs. Commanders and staffs of Army headquarters serving as joint task force or multinational headquarters should also refer to applicable joint or multinational doctrine concerning 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 United States, international, and, in some cases, host-nation laws and regulations. Commanders at all levels ensure their Soldiers operate in accordance with the law of war and the rules of engagement. (FM 27-10)

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 United States Army Reserve unless otherwise stated.

The proponent of FM 6-02 is the United States Army Signal Center of Excellence. The preparing agency is the Signal Center Doctrine Branch, United States Army Signal Center of Excellence. Send comments and recommendations on a Department of the Army (DA) Form 2028 (Recommended Changes to Publications and Blank Forms) to Commander, U.S. Army Signal Center of Excellence and Fort Gordon, ATTN: ATZH-DT (FM 6-02), 506 Chamberlain Avenue, Fort Gordon, GA 30905-5735; by E-mail to usarmy.gordon.sigcoe.mbx.gord-fg-doctrine@mail.mil.

Introduction

"The network is essential to a 21st Century Army. Networked organizations improve the situational awareness and understanding leaders need to act decisively at all points along the spectrum of conflict, while providing connectivity down to the individual Soldier. The network allows dispersed Army organizations to plan and operate together, and provides connectivity to joint, [coalition], and interagency assets."

Secretary of the Army – 25 February 2010

Field Manual (FM) 6-02, Signal Support to Operations, is the premier Signal doctrine publication, and only field manual. FM 6-02 compiles Signal Corps doctrine into three chapters with supporting appendices that address network operations in support of mission command and unified land operations and the specific tactics and procedures associated with organic and nonorganic Signal forces. The fundamental idea of Signal Corps tactics is the employment and ordered arrangement of Signal forces in a supporting role to provide LandWarNet across the range of military operations. The detailed techniques regarding the ways and methods to accomplish the missions, functions or tasks of the Signal Corps indicated in this FM will be addressed in supporting Army techniques publications (ATPs).

Army forces operate worldwide and require a secure and reliable communications capability that rapidly adapts to changing demands. Technological advances improve the capability to fulfill this requirement and an increased dependence to modify, exchange, and store information in cyberspace. Technical networks enable every mission from training the force to the execution of all tasks in order to influence the environment. Technical networks are the voice, data, and video connectivity infrastructure supporting current and future operations. Today's tactical radio systems have the capability to pass digital information and are part of the information environment, expanding the network and increasing the amount of information transported securely.

The Army typically integrates with the joint community, other government agencies, multinational partners, host nations, civil authorities, and other organizations. Extending the network is a capability provided by the Signal Regiment for commanders and staffs to communicate with all necessary entities for mission success, whatever the mission and whomever the partner.

Signal Soldiers are a flexible, integrated, and adaptive force that supports and enables all warfighting functions providing depth in communication and synchronization between organizations both horizontally and vertically. Signal professionals are technically proficient Soldiers able to install operate, defend, and maintain a redundant, robust and secure network using complex systems and equipment.

Improvements in technology permit better use of the electromagnetic spectrum using various waveforms and detailed frequency management. The secure network operates within the constraints of the electromagnetic spectrum. When properly managed, operational and technical communications security advancements provide a secure environment for passing critical information during mission execution at all levels.

FM 6-02 is a new publication and captures tactics and procedures from previous field manuals. This manual supersedes or rescinds appropriate publications after the corresponding Army technique publication approvals.

FM 6-02 chapters include—

Chapter 1 addresses the Signal Corps' support to unified land operations to include warfighting functions, decisive actions, joint missions, space operations, Special Operations, cyberspace and cyber electromagnetic activities, knowledge management, and port and base camp operations. Signal support to space operations focuses on space-based capabilities and systems such as global positioning satellites and satellite communications. Signal Support to Special Operations identifies the unique capabilities provided to support Special Forces and Rangers. Signal support to cyberspace operations discusses planning, engineering, installing, integrating, operating, maintaining, and defending the Army's portion in this global domain and support to cyber electromagnetic activities. Signal support to knowledge management includes information management as an enabler to knowledge management. Signal support to operations also focuses on the functions, services, and support necessary for port and base camp operations communication requirements. Included in this chapter are the Signal core competencies and essential capability.

Chapter 2 outlines the organizational structure and the roles and responsibilities of the Signal organizations that support the Army and joint forces at all echelons. It addresses the roles of the J-6/G-6/S-6 staff sections that serve at the various echelons within Army commands, direct reporting units, joint task forces, government agencies, or non-governmental organizations. It addresses the key capabilities and functions that Signal units provide to Army expeditionary units and joint task forces that execute combat missions across the conflict continuum. This includes the Network Enterprise Centers, theater strategic signal brigades, signal command (theater), brigade combat teams signal company, expeditionary signal battalion, theater tactical signal brigade, and theater strategic signal battalion units that provide signal support throughout the operational theater.

Chapter 3 describes LandWarNet as an enterprise network mission command enabler. LandWarNet is the network in which the operational Army and generating forces operate throughout all phases, in all geographical environments. This chapter addresses the Department of Defense information network and LandWarNet; LandWarNet network transport and information services; Department of Defense information network and LandWarNet network operations; and cyber threats. The chapter also discusses how the Signal Corps' core competencies and essential capability support the secure network and its cloud computing environment.

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

Introductory table. New Army terms

Term	***Remarks***
spectrum management operations	Replaces electromagnetic spectrum management operations

Pro Patria Vigilans! (Watchful for the Country)

Signal Regiment Motto

This page intentionally left blank.

Chapter 1

Signal Support to the Army

As the Army continues to operate in the information age, communication systems become more capable and complex. Signal provides the Army with highly skilled personnel at all echelons to install, operate, maintain, and protect information on the network every commander depends upon. The planning, preparation for, execution and assessment of Signal support to operations is the role of the Signal Soldier. The technical network for unified land operations is essential to the success of the Army's mission. This chapter describes the support to unified land operations and introduces the Signal core competencies.

SECTION I – SIGNAL IN UNIFIED LAND OPERATIONS

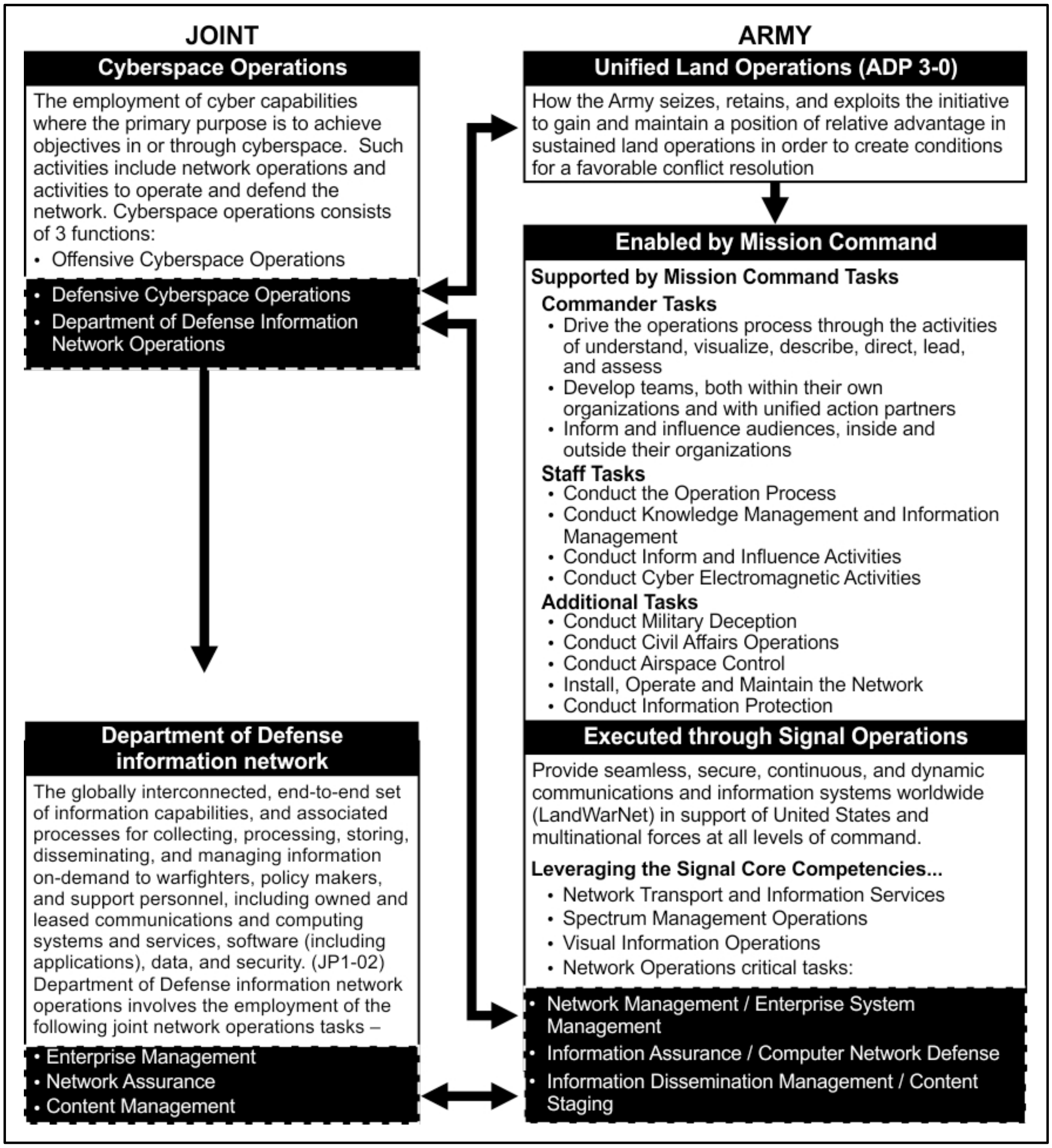
1-1. The Signal Corps' mission is to provide seamless, secure, continuous, and dynamic communications and information systems and visual information support worldwide in support of United States and multinational forces at all levels of command. Signal supports unified land operations by employing unique net-centric capabilities at every echelon, providing secure connectivity to the network and information services. This support is essential to the success of unified land operations and accomplishment of decisive action tasks and directly supports the mission command warfighting function.

1-2. Commanders have a flexible and robust network at their disposal during all types of operations and missions. The network is the primary conduit of information and is used to control forces. The current network architecture allows collaboration among commanders, staffs, and unified actions partners to clarify the meaning of events or situations embedded in their unique and continually evolving operational environment.

SUPPORTING WARFIGHTING FUNCTIONS

1-3. Signal supports all of the warfighting functions directly by engineering, installing, operating, maintaining, and defending the network. Each of the warfighting functions depend on a secure communications infrastructure called LandWarNet. ***LandWarNet* is the Army's portion of the Department of Defense information networks. It is a technical network that encompasses all Army information management systems and information systems that collect, process, store, display, disseminate, and protect information worldwide**. LandWarNet is a network for application of the warfighting functions of mission command, intelligence, fires, sustainment, protection, and movement and maneuver to use for operations and to provide the commander and staff information necessary to make decisions. LandWarNet is part of, and operates in, the cyberspace domain, with network operations (NetOps) supporting both the joint and Army portions of the domain (Figure 1-1, page 1-2). *Cyberspace* is a global domain consisting of the interdependent network of information technology infrastructure and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 1-02). The Army supports the cyberspace operations tasks of defensive cyberspace operations and Department of Defense information network operations by executing LandWarNet NetOps tasks.

1-4. The commander integrates the warfighting functions by executing mission command. The network, with its associated information management and information systems, is the necessary technical infrastructure on which to collect, process, store, display, disseminate and protect information. LandWarNet is the technical network of the mission command system connecting people and enables the sharing of resources and information.



JOINT

Cyberspace Operations

The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such activities include network operations and activities to operate and defend the network. Cyberspace operations consists of 3 functions:

- Offensive Cyberspace Operations
- Defensive Cyberspace Operations
- Department of Defense Information Network Operations

Department of Defense information network

The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, and security. (JP1-02) Department of Defense information network operations involves the employment of the following joint network operations tasks –

- Enterprise Management
- Network Assurance
- Content Management

ARMY

Unified Land Operations (ADP 3-0)

How the Army seizes, retains, and exploits the initiative to gain and maintain a position of relative advantage in sustained land operations in order to create conditions for a favorable conflict resolution

Enabled by Mission Command

Supported by Mission Command Tasks

Commander Tasks

- Drive the operations process through the activities of understand, visualize, describe, direct, lead, and assess
- Develop teams, both within their own organizations and with unified action partners
- Inform and influence audiences, inside and outside their organizations

Staff Tasks

- Conduct the Operation Process
- Conduct Knowledge Management and Information Management
- Conduct Inform and Influence Activities
- Conduct Cyber Electromagnetic Activities

Additional Tasks

- Conduct Military Deception
- Conduct Civil Affairs Operations
- Conduct Airspace Control
- Install, Operate and Maintain the Network
- Conduct Information Protection

Executed through Signal Operations

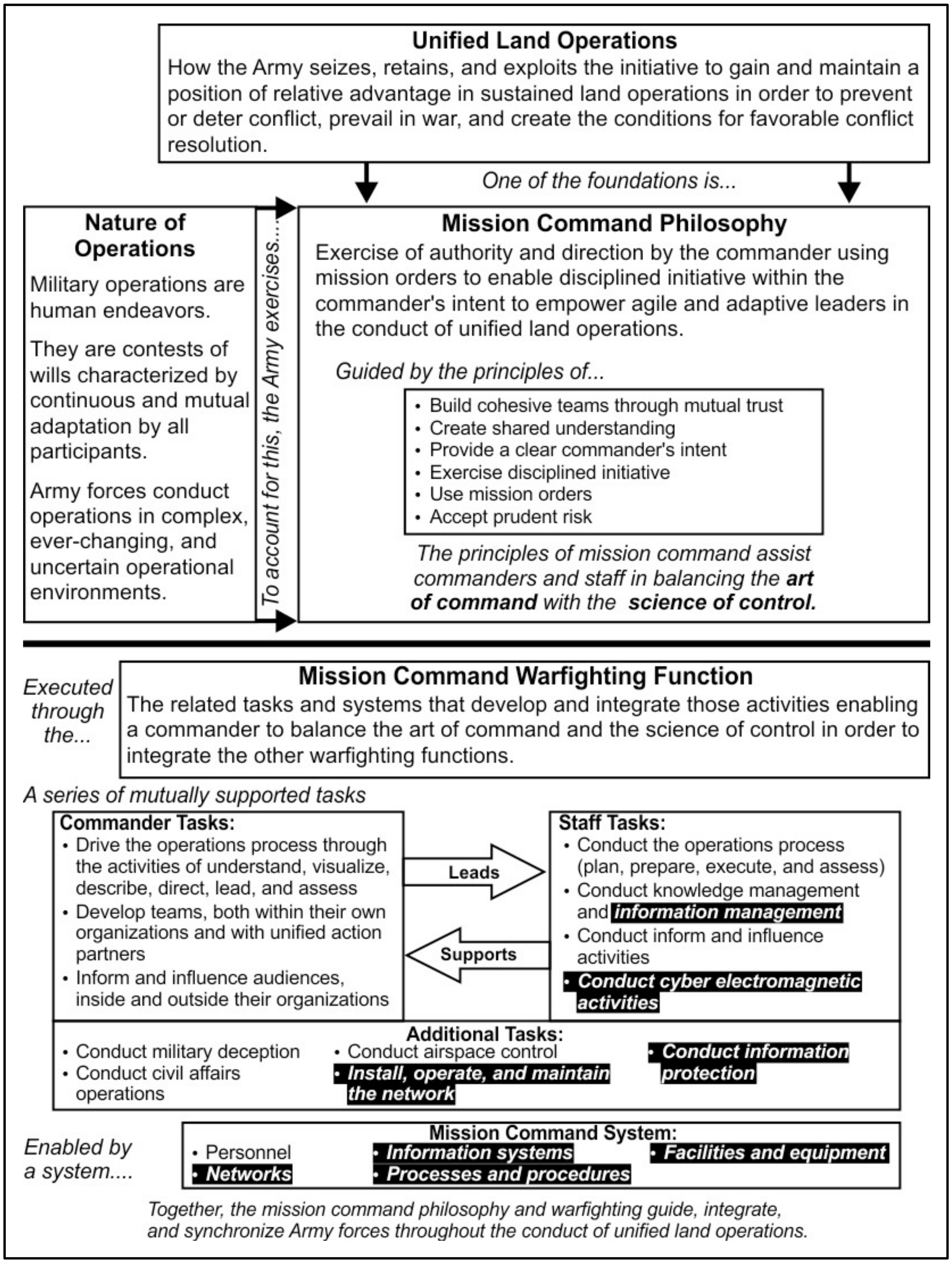
Provide seamless, secure, continuous, and dynamic communications and information systems worldwide (LandWarNet) in support of United States and multinational forces at all levels of command.

Leveraging the Signal Core Competencies...

- Network Transport and Information Services
- Spectrum Management Operations
- Visual Information Operations
- Network Operations critical tasks:
- Network Management / Enterprise System Management
- Information Assurance / Computer Network Defense
- Information Dissemination Management / Content Staging

Figure 1-1. Signal in unified land operations

1-5. Signal support to operations enables or supports the execution of all commander, staff and additional tasks under mission command. The Signal Corps has direct responsibility to install, operate, and maintain the network, support cyber electromagnetic activities, and perform tasks associated with information management and information protection (Figure 1-2). The network enables the integration of the warfighting functions, allowing the commander to access critical information to make decisions and provides communications to control forces. Signal support to operations is an integral part of the mission command system.



Unified Land Operations

How the Army seizes, retains, and exploits the initiative to gain and maintain a position of relative advantage in sustained land operations in order to prevent or deter conflict, prevail in war, and create the conditions for favorable conflict resolution.

One of the foundations is...

Nature of Operations

Military operations are human endeavors.

They are contests of wills characterized by continuous and mutual adaptation by all participants.

Army forces conduct operations in complex, ever-changing, and uncertain operational environments.

To account for this, the Army exercises....

Mission Command Philosophy

Exercise of authority and direction by the commander using mission orders to enable disciplined initiative within the commander's intent to empower agile and adaptive leaders in the conduct of unified land operations.

Guided by the principles of...

- Build cohesive teams through mutual trust
- Create shared understanding
- Provide a clear commander's intent
- Exercise disciplined initiative
- Use mission orders
- Accept prudent risk

The principles of mission command assist commanders and staff in balancing the ***art of command*** *with the* ***science of control.***

Executed through the...

Mission Command Warfighting Function

The related tasks and systems that develop and integrate those activities enabling a commander to balance the art of command and the science of control in order to integrate the other warfighting functions.

A series of mutually supported tasks

Commander Tasks:

- Drive the operations process through the activities of understand, visualize, describe, direct, lead, and assess
- Develop teams, both within their own organizations and with unified action partners
- Inform and influence audiences, inside and outside their organizations

Staff Tasks:

- Conduct the operations process (plan, prepare, execute, and assess)
- Conduct knowledge management and ***information management***
- Conduct inform and influence activities
- ***Conduct cyber electromagnetic activities***

Additional Tasks:

- Conduct military deception
- Conduct civil affairs operations
- Conduct airspace control
- ***Install, operate, and maintain the network***
- ***Conduct information protection***

Enabled by a system....

Mission Command System:

- Personnel
- ***Networks***
- ***Information systems***
- ***Processes and procedures***
- ***Facilities and equipment***

Together, the mission command philosophy and warfighting guide, integrate, and synchronize Army forces throughout the conduct of unified land operations.

Figure 1-2. Signal Corps responsibilities

1-6. Integration of the warfighting functions relies on the network for the capability to inform the commander and staff. This includes the sharing of information among the six functions for each to complete their own missions or tasks. The warfighting functions are mutually supportive and as information passes from one element to another, the network supports the completion of missions in support of the commander’s intent.

1-7. As information and communication requirements change due to the operational and mission variables, the signal element providing support adapts the network to continue supporting and enabling the integration of all warfighting functions. This capability for the network to support changes requires planning and possibly additional resources. Including signal support early in the planning process allows for the relied upon network to properly support all communications. It is vital that the commander include signal support early in the planning process to take full advantage of organic network capabilities and request additional resources as required.

1-8. The flexibility of the network allows scalability to support the commander's requirements as additional units enter or leave an operational area. The Signal Corps expands, extends or contracts the network based on mission requirements. The signal element plans for the appropriate support based on commander's intent and the environmental and mission variables.

SUPPORT TO JOINT OPERATIONS

1-9. Signal operations support communications to joint force commanders, the joint staff, and unified action partners, as required, by providing the network to enable command and control (JP 6-0). Signal Soldiers support the joint communications system, which is the joint force commander's tool to assimilate information and to exercise authority and direct forces over large geographic areas and a wide range of conditions. Just as the network integrates the warfighting functions, effective command and control uses the reliable and secure network to integrate the joint force components.

1-10. During joint operations support, executing the three network operations tasks of enterprise management, network assurance, and content management provides the joint force commander the ability to effectively plan, conduct and sustain operations. Through these tasks, the joint commander has access to cyberspace, service component networks, unified action partners, and higher and lower echelons.

1-11. To support the joint force commander, it is imperative to have communications with all unified partners in all aspects of joint operations. Including the signal support element as early as possible in the planning process is imperative as the interoperability with unified partners adds a level of complexity. The network support is scalable and flexible, and as an operation progresses, the network changes as well to support the commander's intent.

SUPPORTING DEFENSE SUPPORT OF CIVIL AUTHORITIES AND HOMELAND DEFENSE

1-12. The support to the decisive action tasks of offense, defense and stability employ similar network capabilities and the commander's intent is the basis for support requirements. The commander executes mission command and the network integrates all the warfighting functions. Defense support of civil authorities includes unique network requirements from the other decisive action tasks, which need planning to ensure the commander has the appropriate communication assets.

1-13. The Signal Corps provides communication support assets for the protection of United States sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression or other threats as directed by the president or during times of support to civil authorities. The Signal Corps conducts operations in air, land, maritime, space and cyberspace domains. The Department of Defense (DOD) is the primary federal agency for Homeland Defense. The Army dedicates signal assets to Defense Chemical, Biological, Radiological, and Nuclear Response Force and Command and Control Chemical, Biological, Radiological, and Nuclear Response Element-Army on a rotational basis, usually annually. The communication requirements for defense support of civil authorities and homeland defense are similar and require additional planning compared to other missions.

1-14. The disparity of communications systems, use of allocated bandwidth (both civilian and military), and limited interoperable systems hinder the capability of collaborative incident management and response when conducting defense support of civil authorities and Homeland Defense. The allocated signal support to these operations conduct planning and coordination with unified action partners, which may include other military departments, federal and state government agencies, local authorities and officials, and non-governmental organizations. The signal support to homeland defense and defense support of civil authorities is responsible for interoperating with various communication mediums, such as network interfaces including military web portals accessible by non.mil domains, unclassified defense collaborative tool suite, joint task force (JTF)-owned deployable commercial voice switching, secure video teleconferences (VTCs), radio cross-banding of land mobile radios, tactical satellite radios, high frequency radios, and cell phones.

1-15. Designated Army Service command components (ASCCs) provide a signal communications task force capable of assisting federal emergency support to state and local governments during and after a disaster. The task force consists of a communications vehicle; three communications support emergency response vehicles and Signal Soldiers specializing in satellites, networks, and communications systems. These vehicles provide secure and non-secure voice, data communications and a conference room for VTCs when other networks are unavailable. The task force may request more communication assets to complete the mission.

> ***Note***. Refer to JP 3-27, *Homeland Defense*, and ADP 3-28, *Defense Support of Civil Authorities*, for additional information.

SIGNAL SATELLITE COMMUNICATIONS CAPABILITIES

1-16. Satellite communications (SATCOM) is a key means of information transport for unified land operations. SATCOM systems provide a long-haul capability, redundant paths for tactical communications, communications on the move, beyond line of sight communications, and flexibility when preparing the signal plan. Satellite communication systems are located at every echelon in the Army and support the mission command warfighting functions. Supporting intra-theater communications and connectivity to DODIN with SATCOM provides critical services that route through the Defense Satellite Communications System, and the Wideband Global SATCOM constellation. The services include the Defense Switched Network (DSN), Defense Red Switch Network (DRSN), Defense Messaging System, VTC, Telemedicine, SECRET Internet Protocol Router Network (SIPRNET), Nonsecure Internet Protocol Router Network (NIPRNET), and the global mission networks

1-17. A unique signal battalion performs planning, management, monitoring and control of select DOD satellite communications resources. Specially trained Signal Soldiers, which require completion of additional satellite control training, perform these missions. The signal battalion (satellite control) provides SATCOM transmission control and satellite payload control of the Defense Satellite Communications System and Wideband Global SATCOM constellations and space situational awareness. The battalion operates and maintains Wideband Satellite Operation Centers and a Defense Satellite Communications System Operations Control Certification Facility. Operating these centers enables communications for the Commander in Chief, Secretary of Defense, Chairman of the Joint Chiefs of Staff, Armed Services, State Department, intelligence activities, combatant commanders, and allied forces during unified actions.

1-18. The signal battalion (space control) supports unified land operations by performing the following functions—

- Monitor and control functions for tactical and strategic use of Defense Satellite Communications System and Wideband Global SATCOM satellites.
- Transmission and payload control of assigned Defense Satellite Communications System and Wideband Global SATCOM satellites.
- Payload command and telemetry functions.
- Electromagnetic interference detection and geo-location.
- Space situational awareness.
- 24-hour communications service to DOD agencies and Soldiers.
- Satellite configuration control.
- Satellite link establishment.
- Maintenance of link quality.
- Transmissions power management.
- Monitor electromagnetic spectrum.
- Monitor satellite terminals.
- Terminal positive control and subnet work control.

1-19. The Signal officer with responsibilities of signal operations at each echelon tracks the status of all satellite constellations affecting the organization’s mission, develop the signal plan, and provide Soldiers with required mission capabilities. The Signal officer obtains space weather reports from the Air Force Weather Agency and Army Space Support Elements to advise the commander on how space weather affects the organization's ability to utilize network systems.

> ***Note***. Refer to FM 3-14, *Space Operations*, for additional information.

SPECIAL OPERATIONS SIGNAL SUPPORT

1-20. The United States Army Special Operations Command provides trained and ready special forces, ranger, special operations aviation, military information support operations, and civil affairs personnel to geographic combatant commanders (GCCs) and U.S. diplomatic consulates. These special operations forces require seamless industry standard and protocol-compliant voice, data, and imagery support. There is special operations communications support at all echelons, from the national level to the unit level. The special operations communications networks need to include redundant routes to prevent site isolation. They must also take advantage of automated systems that provide transparent connectivity to the user. The communications system must exploit all available means, including host nation assets, to provide robust and ready access to the Department of Defense information network in support of Army Special Operations Forces.

1-21. The Signal Battalion (Special Operations) (Airborne) deploys scalable teams capable of providing worldwide, innovative, responsive, reliable and assured capable communications support to special operation forces and theater special operations forces. On order, provides theater mobile strategic special operations forces entry points and global NetOps.

1-22. The Signal Battalion (Special Operations) (Airborne) provides the following capabilities—

- Theater enterprise level network planning, engineering, architecture determination/integration.
- Critical dual-homing capability.
- The planning, engineering, installation, operation, maintenance, and defense for theater of operations level special operations forces communications systems.
- Special operations forces theater network communications infrastructure is uniform, pervasive, and centrally managed.
- Signal nodes to provide initial, early entry, and sustained secure communications systems providing voice, video, and data at required classification levels for U.S. Army Special Operations Command headquarters performing functions as a forward-deployed JTF.
- Coordinate operations within the theater level NetOps configuration management program.
- Administer and direct execution of NetOps within the theater of operations.
- Install, operate, maintain, and control the communications systems providing voice, video, and data in support of the regional theater special operations command commanders.
- Communications security (COMSEC) account management and maintenance.
- Sustainment and field level maintenance to organic signal equipment, automation systems, and limited maintenance to special operations forces peculiar signal equipment.
- Communications support for airborne and airdrop operations.

RANGER REGIMENT SIGNAL SUPPORT

1-23. The Signal Company, Ranger Regiment deploys worldwide to install, operate, maintain and protect the regiment's mission command systems. The Signal Company, Ranger Regiment establishes networks that support the regiment’s operations and integrate with coalition forces land component command/Army force, signal support for the ranger battalions, the Ranger Special Troops Battalion, and the Headquarters, Headquarters Company, Ranger Regiment. The Signal Company, Ranger Regiment establishes networks that support the regiment’s operations and integrates with coalition forces land component command/Army force.

1-24. The Signal Company, Ranger Regiment provides the following capabilities to support the unit's mission—

- Network transport and information services to support maneuver, support and mission command elements.
- Tactical radio relay, retransmission and beyond line of sight high frequency and satellite communications capabilities to extend networks.
- Global Broadcast Service with the ability to receive high bandwidth products such as imagery, logistics data, and digital map information to supporting mission command systems.

Note. Refer to FM 3-05.160, *Army Special Operations Forces Communications System*, for additional information.

SIGNAL ROLE IN CYBERSPACE AND CYBER ELECTROMAGNETIC ACTIVITIES

1-25. Signal support to operations executes the tasks to engineer, install, operate, maintain and defend the network. LandWarNet is part of the Department of Defense information networks (DODIN) and both are part of the domain called cyberspace, in which DOD networks operate. The Signal Corps supports and coordinates Army cyberspace operations with national and joint cyberspace operations. Cyberspace operations consist of offensive cyberspace operations, defensive cyberspace operations, and Department of Defense information network operations.

1-26. The Signal Regiment, through its core competencies of network operations, network transport and information services, and spectrum management operations (SMO), executes Department of Defense information network operations on LandWarNet. *Department of Defense information network operations* are the operations to design, build, configure secure, operation, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information networks (JP 1-02). These include proactive technical functions such as configuration control, system patching, information assurance (IA) measures and user training, physical security, secure architecture design, operation of host-based security systems and firewalls, and encryption of data at rest. Many Department of Defense information network operations activities are regularly scheduled events and the aggregate effect establishes the security framework on which all missions ultimately depend.

1-27. *Defensive cyberspace operations* are passive and active operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems (JP 1-02). To facilitate defensive cyberspace operations, Signal personnel apply NetOps and SMO capabilities and processes in real-time to detect, analyze, and mitigate threats and vulnerabilities, as well as outmaneuver adversaries in order to defend LandWarNet, protect critical missions, and enable freedom of action. To defend cyberspace, Signal personnel work to detect, analyze, and respond to unauthorized activities not detected by routine measures. This requires Signal personnel are aware of timely intelligence and threat indicators from traditional and advanced sensors, vulnerability information from DOD and non-DOD sources, and accurate effects assessment information from offensive cyberspace operations and Department of Defense information network operations.

1-28. Working in concert with the Department of Defense information network operations and defensive cyberspace operations aspects of Signal core competencies, offensive cyberspace operations allows operational offensive planners the ability to coordinate and synergize efforts in and through cyberspace, as well as other domains necessary to support the accomplishment of the commander's objectives. *Offensive cyberspace operations* are operations intended to project power by the application of force in or through cyberspace (JP 1-02). Offensive cyberspace operations use cyberspace attack and cyberspace information collection capabilities to deny access by disrupting, degrading, or destroying the ability of the adversary to use cyberspace. Although signal organizations do not conduct offensive cyberspace operations, through the performance of their defensive cyberspace operations mission the signal units may be able to detect and attribute external threat activity on friendly networks. Signal organizations must be able to support entities that can execute offensive cyberspace operations.

1-29. Cyber electromagnetic activities include cyberspace operations, SMO and electronic warfare. Cyber electromagnetic activities are leveraged by commanders to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum. These activities ensure information availability, protection, and delivery as well as a means to deny, degrade, or disrupt the enemy's use of its' command and control systems and other cyber capabilities. Commanders use information and a mission command system to understand, visualize, describe, and direct operations (ADRP 3-0). To support cyber electromagnetic activities at the ASCC level and below, G-6/S-6 and spectrum managers integrate, synchronize, and coordinate NetOps and spectrum management actions with mutually supporting capabilities that reside within the G-2/S-2 and G-3/S-3.

Note. Refer to Army doctrine on Cyber Electromagnetic Activities (CEMA), for additional information.

ENABLING KNOWLEDGE MANAGEMENT

1-30. *Information management*, the science of using procedures and information systems to collect, process, store, display, disseminate, and protect data, information, and knowledge products, enables knowledge management functions. *Knowledge management* is the process of enabling knowledge flow to enhance shared understanding learning and decisionmaking (ADRP 6-0). Knowledge management (KM) facilitates the transfer of knowledge between staffs, commanders, and forces. Knowledge management aligns people, processes, and tools within an organization to distribute knowledge and promote understanding. Signal enables KM by providing network architecture and the technological tools necessary to support content management and knowledge sharing.

1-31. Mission Command Center of Excellence has primary responsibility for knowledge management. Signal support enables KM by providing network operations and information management support, both through the G-6/S-6 and by serving in various positions in the KM section. Knowledge management identifies the specific roles and responsibilities for positions in the KM Section. The table of organization and equipment identifies what positions Soldiers may serve in KM sections in various unit types and echelons.

1-32. Signal Soldiers assigned to the KM section ensure that the unit's information systems network support knowledge creation, and incorporate automated KM tools. They perform information management tasks that include application and database administration, data backup and migration, website interface maintenance, troubleshooting, security, and configuration.

Note. Refer to FM 6-01.1, *Knowledge Management Operations*, for additional information.

SUPPORT TO PORT OPERATIONS

1-33. The U.S. Transportation Command's Transportation Command, Control, Communications, and Computer Systems is responsible for the Integrated Data Environment Global Transportation Network Convergence system. The Integrated Data Environment Global Transportation Network Convergence system provides the integrated transportation data and systems necessary for U.S. Transportation Command to effect the synchronization of mission command warfighting function tasks, planning and analysis, and business operations in tailoring customer requirements.

1-34. The respective ASCC G-6 coordinates with their GCC and supports the communications operations for the harbormaster detachment, which is responsible for coordinating and synchronizing vessel operations. When the detachment arrives, it establishes the harbormaster command and control center and the necessary radio communications and weather data sensors. One of the duties of the command and control center is to establish communications with vessels.

Note. Refer to ATTP 4-15, *Army Water Transportation Operations*, for additional information.

SUPPORT TO BASE CAMP COMMUNICATIONS

1-35. Base camp size, level of capabilities and purpose determine requisite signal support. Operational needs of tenant and transient units determine the level of signal support.

1-36. When an G-6/S-6 and/or signal organization has the responsibility to provide signal support to a base camp, the respective G-6/S-6 coordinates with the base camp commander to identify communications requirements, and coordinate communications operations with sister services as necessary.

Note. Refer to ATP 3-37.10, *Base Camps*, Appendix D, *Signal Support to Base Camps*, for additional information.

SECTION II – SIGNAL CORE COMPETENCIES

1-37. The Signal Corps supports the Army, joint services, and multinational partner missions by executing the Signal core competencies and executing the essential capability. The core competencies are network operations, network transport and information services, spectrum management operations, and visual information operations. COMSEC is an essential capability of signal support but not considered a core competency. The core competencies and essential capability enable the warfighting functions and their integration through the transport, security, storage, display, information management, integration, and maintenance of the network.

NETWORK OPERATIONS

1-38. *Network operations* are the activities conducted to operate and defend the Department of Defense information networks (JP 6-0). The Army conducts NetOps for LandWarNet, and other networks as required, and for the purpose of this field manual, use of the term NetOps specifically refers to related activities on all applicable networks.

Note. Refer to Chapter 3 for additional information on network operations.

NETWORK TRANSPORT AND INFORMATION SERVICES

1-39. Network transport and information services are the combined physical assets and activities to ensure that data reliably transverses the network and is available as information to the user. ***Network transport* is a system of systems including the people, equipment, and facilities that provide end-to-end communications connectivity for network components**. Information services enable the planning, controlling, and manipulating of information throughout its lifecycle. They include, but are not limited to, web services, E-mail, common directories, search services, and data services. Information services allow forces to access, store, and share information among unified action partners and civilian organizations, as well as dynamically tailor and prioritize information requirements to support the mission and affect the operational environment. The resources to connect the clients may belong to U.S. Services or forces, non-U.S. Services or forces, host nation or commercial assets.

Note. Refer to Chapter 3 for additional information on network transport and information services.

SPECTRUM MANAGEMENT OPERATIONS

1-40. ***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.** The objective of Army spectrum management operations (SMO) is to ensure access to the frequency spectrum in order to support commanders during unified land operations.

1-41. Spectrum management is the planning, coordinating, and managing use of the electromagnetic spectrum through operational, engineering, and administrative procedures. The objective is coordinated, prioritized, and deconflicted operations for electromagnetic spectrum-dependent systems without causing or suffering unacceptable interference. The coordination for spectrum use may be with government or civil authorities. Spectrum management also includes enforcing, identifying, and eliminating unauthorized use of the frequency spectrum.

1-42. Frequency assignment entails the requesting and issuance of authorization to use frequencies for specific equipment. Frequency assignment may include providing the frequencies for assignment to a combat net radio network, providing frequencies for unmanned aerial systems, or providing the frequencies for assignment to a line of sight (LOS) network. SMO includes managing frequencies down to the brigade level for all equipment that operate using the electromagnetic spectrum.

1-43. Host nation coordination is obtaining authorization to operate electromagnetic spectrum–dependent systems within a sovereign nation. This constitutes conforming to international and national laws on a regular basis in addition to safety of life issues. This coordination is imperative to the conduct of unified land operations as the joint force commanders, subordinate commanders or the operators may be criminally or financially liable for violations and may have equipment confiscated.

1-44. SMO includes defining policies and ensuring adherence to policies while supporting commanders. Failure to adhere to these policies and regulations may lead to mission failure, equipment damage, fines and loss of life.

Note. Refer to JP 6-01, *Joint Electromagnetic Spectrum Management Operations*, for additional information.

VISUAL INFORMATION/COMBAT CAMERA

1-45. *Visual information* is the use of one or more of the various visual media with or without sound (CJCSI 3205.01C). Generally, visual information includes still photography, motion picture photography, video or audio recording, graphic arts, visual aids, models, displays, visual presentation services, and the support processes. Combat camera (COMCAM) is a specific mission within visual information. COMCAM supports the commander by acquiring, processing, and distributing classified and unclassified still and motion imagery collected during ongoing military operations.

1-46. The mission of visual information activities and Soldiers is to acquire and provide the president, Office of the Secretary of Defense, joint staff, military departments, and Army commanders with record documentation, multimedia/visual information products, and services to satisfy official requirements. Security classification, operations security or subject sensitivity does not prevent visual information documentation. Visual information documentation is the process of using motion media, still photography, and audio equipment to acquire audio and visual records of events activities since classification regulations also apply to visual information products.

1-47. The official requirements, which visual information Soldiers can provide support to may include, but are not limited to, mission command warfighting tasks, training, education, logistics, human resources, special operations, information operations, military information support operations, public affairs, and intelligence to effectively convey accurate integrated intelligence to the Soldier, decisionmakers, and supporting organizations. However, because these Soldiers have specific missions that require special training, augmentation is limited to providing COMCAM support, which a commander requests and for which the visual information Soldier is equipped and trained. Visual information Soldiers may be required to perform dedicated visual information capabilities to support medical, safety, and criminal investigation.

1-48. Visual information support is limited to official events or activities. Establish the priority for visual information support with consideration to mission, cost effectiveness, the quality and quantity of products and services available. The use of visual information products, equipment, or facilities for other than official purposes, such as loaning equipment to local and state governments or nonprofit organizations meeting on government property, is at the discretion of the local commander in accordance with Army Regulation (AR) 700-131, AR 735-5 and AR 25-1.

1-49. COMCAM requirements are different from public affairs and press pool media requirements. While combat imagery may be used for public affairs purposes, its primary use is as an operational decisionmaking tool. COMCAM personnel have access to information and areas to which media personnel may not have access. COMCAM personnel photograph all aspects of an operation or event. Intelligence, operations, and public affairs staff coordination decide classification, sensitivity, and public release to the media.

1-50. Tactical COMCAM documentation is an essential resource that supports all elements of operations at all levels of war. They share documentation, as required, to support the operational and planning requirements of commanders and decisionmakers from the combatant commanders through the president and Secretary of Defense. It is a fundamental tool of commanders and decisionmakers that, when utilized properly, is an effective combat force multiplier. COMCAM capabilities include the following—

- Static line and free fall jump qualified COMCAM equipped personnel.
- COMCAM personnel qualified and equipped to centrally manage process and distribute classified and unclassified imagery to support joint operations.

Note. Refer to FM 6-02.40, *Visual Information Operations*.

COMMUNICATIONS SECURITY

1-51. *Communications security* is the component of information assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptographic security, transmission security, emissions security and physical security of COMSEC material (CNSSI No. 4009). The Signal Corps deems COMSEC an essential capability, as Signal assets routinely perform all other respective tasks to secure joint and Army electronic communications and those with COMSEC accounts have the capability to generate National Security Agency (NSA) approved key.

1-52. The need for security cannot override the basic requirement to communicate and there must be a balance. LandWarNet systems and devices use a robust encryption capability that provides IA to all Army forces while ensuring the support of communication services. COMSEC and its respective activities provides for this information protection. Modernized net-centric cryptography is an integral component to achieving DOD warfighting systems objectives. Effective tactical communications also requires the management of keys, devices and other COMSEC material at the lowest echelon possible while maintaining the appropriate physical security level of the equipment and material. This allows for COMSEC managers and operators the ability to react to contingencies such as emergency key supersession, equipment failures, or human error, with minimal downtime. The integration of COMSEC key management products, services, and training into network planning operations is essential to enabling secure net-centric information operations.

1-53. U.S. Army Training and Doctrine Command, through the Signal Corps, is responsible for developing and integrating COMSEC doctrine, consistent with established Army COMSEC policies and procedures. It is the commander’s responsibility to enforce all regulations pertaining to COMSEC. The individual COMSEC user is personally responsible for the physical protection and accountability of all COMSEC material in their possession or control. AR 380-40 provides further guidance on responsibilities for COMSEC.

Note. For more information on COMSEC operations refer to TB 380-41.

This page intentionally left blank.

Chapter 2

Roles and Responsibilities of Signal Organizations

Signal elements support all types of operations. This support requires the signal unit to engineer, install, operate, maintain, and defend communication networks and information services. Most signal units exist to support the Army's needs, whether organic to the unit or pooled assets. However, some signal units provide support to unique missions. The unpredictability, complexity, and inherent dangers of the operational environment require that signal leaders be adaptive, flexible, and technically proficient. Operations can expand or contract in scale, and signal support must be fully responsive to changing conditions. This chapter discusses the roles and responsibilities of organic support at each echelon, those units without organic support, pooled assets, and the units that enable all communications.

SECTION I – UNITS WITH ORGANIC SIGNAL ASSETS

2-1. The roles and responsibilities of Signal commanders, G-6/S-6 and units are to ensure unity and priority of effort in providing baseline services (See Chapter 3, paragraph 3-13) to supported units, and when approved, at the appropriate command authority. This section addresses those roles and responsibilities in units with organic signal assets from the lowest echelon to highest. Each echelon performs the functions of the next lower echelon. Included in the echelons above battalion sections are the additional roles and responsibilities performed, at their respective level.

S-6/G-6 RESPONSIBILITIES

2-2. Commanders and staffs disseminate and share information among people, elements, and places. 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 actions. Action occurs when there is clarity between commanders and subordinates. The S-6/G-6 element facilitates this communication.

2-3. The S-6/G-6 has the following responsibilities at all echelons—

- Ensure the commander can always securely communicate.
- Determine the supportability and feasibility of the signal plans.
- Manage communications assets—
  - Satellite systems.
  - Tactical radios.
  - Networking equipment.
- Determine specific or unique communications and network requirements.
- Consult and inform higher, lower, and adjacent headquarters to ensure efficient communications.
- Identify and validate the assigned unit's information support requirements.
- Recommend site selection of command posts (CPs) and placement of key signal assets to ensure optimal network availability to higher, lower, and adjacent units.
- Write the signal annex to the unit's operation order and fragmentary orders and articulate network tasks to subordinate units required by Army regulatory guidance.
- Coordinate and provide responsive redirection of network priorities, policies, and allocations.
- Manage LandWarNet assets in the area of operations.

- Protect and defend the network by conducting information assurance/computer network defense (IA/CND), to include the submission of DOD Information Assurance Certification and Accreditation Process requirements and IA in compliance with AR 25-1, AR 25-2, and DODI 8500.02.
- Provide oversight of periodic preventive maintenance and services of signal assets within the assigned unit.
- Integrate automated information systems.
- Process requests to connect/operate respective hardware and software that require ports, protocols and services modifications at the top-level architecture.
- Oversee the management and distribution of the respective COMSEC account in accordance with AR 380-5, AR 380-40, and TB 380-41.
- Coordinate to reposition signal equipment within area of operation.
- Coordinate maintenance support for all NetOps, network transport, information services, and spectrum management equipment and applications.
- Recommend essential elements of friendly information.

2-4. Many of the functions of S-6/G-6 are similar at all echelons. The higher echelon S-6/G-6 have the same role of the lower echelon S-6/G-6, with an increase in scope. Each level contains its own unique challenges and opportunities.

BATTALION S-6

2-5. The S-6 integrates automated information systems, manages the network, conducts IA/CND, and coordinates SMO. The primary signal operations planner is also an active member of the operations process. The S-6 ensures the commander can communicate to facilitate effective mission command of their respective units. They determine the supportability and feasibility of the signal plan supporting each course of action being considered during the military decisionmaking process.

2-6. The battalion S-6 section is responsible for the communications assets within the battalion area of operations. They interact closely with the executive officer, operations staff officer (S-3), and other staff officers to determine specific or unique communications and network requirements. They consult higher, lower, and adjacent headquarters to ensure efficient communications employment throughout the battalion area of operations. There is a close relationship between the battalion S-3 and the S-6. The S-6 understands the commander’s plans, thought processes, and an architecture that allows for dynamic tasking to support the mission.

2-7. Each maneuver battalion has organic tactical radios, local area network, and wide area network capabilities. The battalion provides primary internal communications and a command post node from the brigade signal company, which enables wideband beyond line of sight (BLOS) access to the brigade information network and limited Defense Information Systems Network (DISN) services, SIPRNET, NIPRNET, voice, and data services.

2-8. The S-6 maintains an accurate running estimate on the communications capabilities and provides the commander signal support plans for the design and implementation of the battalion’s communications requirements. The S-6 works closely with the S-4 to determine communications combat power and provides the commander with the associated risks.

BRIGADE S-6

2-9. The S-6 section personnel within the brigade CPs support the commander’s communications requirements across the area of operations. The S-6 consults and informs the higher headquarters J-6/G-6, the brigade signal company commander, assigned or attached battalion S6 staffs, and adjacent units to ensure efficient communications employment throughout the brigade area of operations.

2-10. The S-6 is responsible for planning the communications and information systems support for the brigade, brigade CPs, and subordinate units organic to, assigned to, or operating within the brigade area of operations. Unless specifically noted, these roles and responsibilities are applicable to both the brigade combat team (BCT) S-6 and the multifunctional support brigade S-6.

2-11. Although the support provided is the same, the focused number of users among the various systems and the mission requirements are different based upon type of brigade. The coordination for planning network requirements and personnel support remain the same. The S-6 works closely with the S-4 to determine communications combat power and provides the commander with the associated risks. Additional responsibilities of the S6 also include—

- Conduct NetOps for the brigade and subordinate units.
- Conduct SMO for the brigade and subordinate elements.
- Coordinates with and assists the Sustainment Automation Support Management Officer.
- Contribute to the collection and dissemination of relevant information in support of CEMA situational awareness and related common operational picture.
- Manage the operations of the network to ensure information system availability.
- Support cyber electromagnetic activities elements as required.

Brigade Signal Company

2-12. The brigade signal company provides 24-hour communications support of the signal system networks for Stryker brigade combat teams, infantry/armored brigade combat teams, and supported multi-functional support brigades (fires brigades, battlefield surveillance brigades, sustainment brigades). Unit subordinate elements (platoons and teams) deploy throughout the BCT area of operations.

2-13. The brigade signal company provides operational elements designed to engineer, install, operate, maintain, and defend the joint enterprise theater network supporting operations as an integral part of the Coalition Forces Land Component Command/Army forces. It extends DISN services to the division and subordinate elements operating in an area of operation and provides basic network management (NM) capabilities. The brigade S-6 coordinates with the brigade S-3 to request allocation or positioning of signal assets in the brigade area of operations. The unit commander maintains command authority over the company's assigned operational platoons and attached elements. These units provide the following capabilities—

- Connects the brigade to LandWarNet.
- Provides a high-capacity LOS section to communicate between CPs.
- Provides a data support team for networks services, local area network access and use of mission command systems.
- Provides a wireless network extension team for range extension of tactical voice and data radios.
- Usually, one network extension support platoon deploys with the BCT main CP, and one with the brigade support battalion tactical CP.

Division

2-14. The division G-6 is the principal staff officer for all matters concerning communications, NetOps, network transport, information services, and SMO for the division and subordinate or assigned units operating within the division area of operations. The G-6 recommends changes to the network in support of the division commander's intent.

2-15. The G-6 recommends the repositioning of signal equipment within the division area of operations. The division G-6 is responsible for advising the division commander, staff, and subordinate commanders on all aspects related to the network and information service integration to include staff responsibilities, technical guidance, and training readiness.

2-16. The division G-6 controls LandWarNet assets in the division area of operations through the division network operations and security center (NOSC). The NOSC enables the G-6 to monitor the health of the network and direct the management of network faults, configurations, resource allocation, performance, and security in support of the command. When part of a joint task force headquarters, the division NOSC will act as the core of a joint network operations control center.

Division G-6 Responsibilities

2-17. The G-6 controls communications assets in the division AO, and the division NOSC manages those assets. The telecommunications service order process informs subordinate formations of changes to LandWarNet. Accessing LandWarNet requires strict adherence to the directed changes. The timely implementation of directed changes ensures vulnerabilities with known fixes are mitigated or remediated. The NOSC enables the G-6 to monitor the health of the network in support of the command.

2-18. The G-6 is responsible for advising the division commander, staff, and subordinate commanders on communications and information operational matters (staff responsibilities, technical guidance, and training readiness responsibilities).

2-19. The G-6 is accountable for all network transport, network services, COMSEC and the viability of information systems across the division. The G-6 is responsible for the inherited controls of subordinate formations, and provides the following—

- Manages installation and operation of the main and tactical (TAC) CP local area networks.
- Operates and coordinates signal operational networks at the main and TAC CPs.
- Assists division/corps with network installations and troubleshooting as needed.
- Forms the information systems security office.

Division Signal Company

2-20. The division signal company provides 24-hour communications support to the division headquarters. It provides elements designed to engineer, install, operate, maintain, and defend the joint theater network supporting division operations as an integral part of the division, theater army, Army forces, or JTF in accordance with technical guidance provided by the division G-6.

2-21. The division signal company is subordinate to the headquarters and headquarters battalion. The division signal company operates under the direction of the division G-6 for NetOps within the area of operations. The division signal company provides the following—

- NetOps and management facilities to include a network command element, information assurance cell and computer network defense cell.
- COMSEC support via cryptographic equipment, key, and services for the division.

Corps

2-22. The corps G-6 oversees and directs the planning, operations, and coordination of all matters concerning NetOps, network transport, information services, and SMO for the corps headquarters and assigned units. The G-6 is the senior Signal officer in the corps and coordinates with lower, adjacent, and higher echelons of command to ensure adequate network support. When the corps headquarters serves as the headquarters for a joint task force, the corps G-6 becomes the joint task force J-6 unless superseded by a more senior Signal officer.

Corps G-6 Responsibilities

2-23. The corps G-6 has the same roles and responsibilities as mentioned for the division G-6, with a different scope. The corps G-6 is responsible for integrating corps network and information systems, including the training readiness responsibility of the corps signal company. The G-6 is responsible for planning, designing, and directing the corps signal company to execute the communications plan in support of the corps commanders' intent.

2-24. The G-6 employs a fully integrated NOSC to conduct NetOps for the corps commander. The corps NOSC is responsible for establishing the corps information network and provides the operational and technical support to all of the corps signal elements in its area of operations. Like the division NOSC, the corps NOSC enables the G-6 to monitor the health of the network and direct the management of network faults, configurations, resource allocation, performance, and security in support of the command.

Corps Signal Company

2-25. The corps signal company provides flexible and robust communications necessary to support the corps, to include the corps main CP, TAC CP. The signal company specifically provides functions for the corps headquarters only. The signal company provides NetOps and management facilities to include a network command element, information assurance communications network defense, and COMSEC account.

2-26. The corps signal company operates under the direction of the corps G-6, and provides elements designed to engineer, install, operate, maintain, and defend the corps network enterprise systems in support of operations. They direct operational elements designed to engineer, install, operate, maintain, and defend the theater network supporting division and corps operations. The corps signal company also provides the following capabilities—

- NetOps and management facilities to include a network command element, information assurance cell and computer network defense cell.
- COMSEC support via cryptographic equipment, key, and services for the corps headquarters.

SECTION II – UNITS WITHOUT ORGANIC SIGNAL ASSETS

2-27. Army commands, functional brigades, and functional battalions draw signal support from a pool of assets. A pooled asset is a collection of signal units subject to standard requirements code 11 rules of allocation. Units requiring direct support request signal support through command channels. Approval relies upon the recommendation of their supporting J-6/G-6/S-6 staff and the validation of the J-3/G-3/S-3 staff and the orders process.

TYPES OF UNITS WITHOUT ORGANIC SIGNAL ASSETS

FUNCTIONAL SUPPORT BRIGADES

2-28. The Army normally assigns functional brigades to divisions or corps. Examples of functional brigades are military police; engineer; air and missile defense; medical; chemical, biological, radiological, nuclear, and high yield explosives defense; and civil affairs. Functional brigades may be attached or under operational control (OPCON) to a corps or division. Functional brigades do not contain organic signal companies or assets. Pooled assets such as an expeditionary signal battalion (ESB), or the organic assets of the supported unit, provide signal support to functional brigades. The supported unit assumes the responsibility for NetOps requirements and may require augmentation to manage the network.

2-29. The functional support brigade G-6/S-6 establishes and maintains a close relationship with the supported unit's G-6/S-6. The functional brigade G-6/S-6 assesses and defines the level of signal services, capabilities, and support based upon mission requirements. Requests for required services are in accordance with the normal G-3/S-3 orders process. The supporting signal unit provides the required signal support package(s) from pooled assets to satisfy the communications and information exchange requirements. The supporting signal unit often provides a predetermined surplus of signal assets (spares) based upon the unit's operational mission requirements.

TASK FORCES

2-30. At the tactical level, a standing joint force headquarters, combatant command headquarters, combined JTF, or single service task force may perform NetOps functions. Task forces organized by combatant commanders may be a combined JTF (or single service task force) and assign tailored forces, including army signal capabilities. The combined joint task force exercises control of the joint force systems and networks through a joint network operations control center as detailed in CJCSM 6231.01D.

2-31. The Army forces (ARFOR) commands the Army Service portion of the JTF. The ARFOR is directly subordinate to the JTF, but are also under the administrative control of the ASCC. The ARFOR has a dual NetOps reporting relationship to the JTF and the geographical combatant command ASCC. The JTF exercises overall authority and responsibility for NetOps within the ARFOR. The geographical combatant command ASCC also has a responsibility to provide guidance through NetOps channels to the ARFOR to ensure compliance with Army NetOps standards.

ASCC/THEATER ARMY G-6 STAFF STRUCTURE/FUNCTIONS

2-32. The Commander of the signal command (theater) (SC[T]), except in CONUS, is dual-hatted as their respective G6 with a separate G-6 staff that focuses on signal requirements within the theater (Figure 2-1). The G-6/Theater Army G-6 plans, prioritizes, and coordinates requirements and information systems networks to support the theater army. The G-6/Theater Army G-6 coordinates with the GCC for authority to operate within the host nation. The G-6 integrates information systems support to GCC designated joint, multinational, official government organization, and non-official government organization sites. The G-6 assesses the information systems network's ability to meet mission command and information exchange requirements, and develops relevant portions of theater Army operation orders and operation plans. The operations branch consists of the COMSEC, spectrum, and plans and exercise elements.

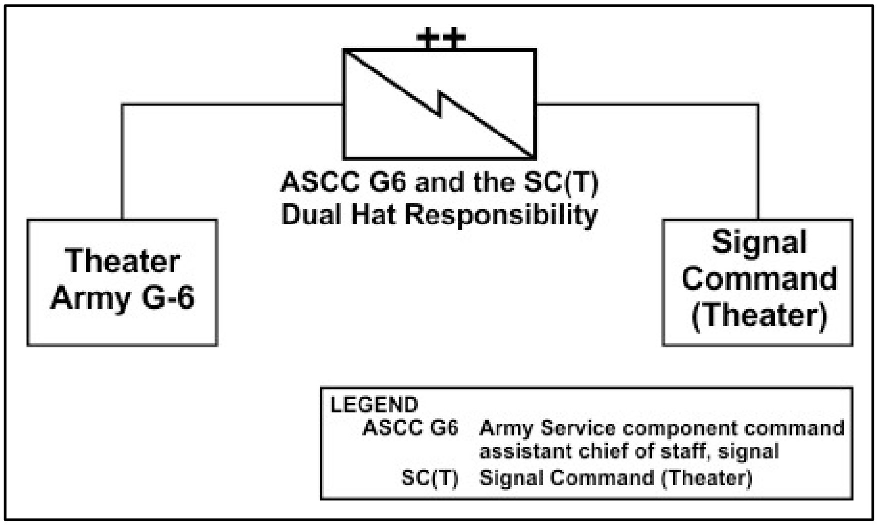

ASCC G6 and the SC(T)
Dual Hat Responsibility
Theater Army G-6
Signal Command (Theater)
LEGEND
ASCC G6 Army Service component command assistant chief of staff, signal
SC(T) Signal Command (Theater)

Figure 2-1. Signal Command (Theater) and Army Service component command G-6 relationship

TYPES OF SIGNAL UNITS LEVERAGED FOR SUPPORT

TACTICAL INSTALLATION AND NETWORKING-ENHANCED COMPANY

2-33. The tactical installation and networking company-enhanced (TIN-E) deploys worldwide to provide network installation utilizing a user-provided bill of material, troubleshooting, quality assurance testing and handoff coordination to enable transition from tactical to semi-permanent automation support for ASCC, GCC, SC(T) commanders and JTF or coalition headquarters.

2-34. The TIN-E provides the following capabilities to support the unit's mission—

- Execution of mission command warfighting function tasks, personnel administration, maintenance and supply functions.
- Technical expertise to interpret and implement engineer implementation plans for communications systems.
- Direction and technical expertise to sections and teams for the restoration of supported facilities.
- Installation, maintenance, and repair of aerial, buried, or underground cable, wire, and fiber optic transmission systems.
- Repair and maintenance of existing cable, wire, and fiber optic systems.
- Antenna and tower construction and repair.

- Connecting various theater HQ local area networks into required wide area network via cabling, hardware installation and connection to tactical and indigenous switches and transport systems.
- Digital system installation to include local area network, network security, hardware, SIPRNET, NIPRNET and VTC.
- Quality assurance testing and handoff of installed and restored systems.

COMBAT CAMERA COMPANY

2-35. The COMCAM company provides day/night still/video acquisition in support of unified land operations.

2-36. The COMCAM company provides combat camera support to joint and U.S. Army operations and exercises as directed by the combatant commanders. The company provides COMCAM documentation to support the decisionmaking process for field commanders, the Joint Chiefs of Staff, DOD, President and the Secretary of Defense. The COMCAM company provides the following capabilities to support the unit's mission—

- Execution of mission command warfighting function tasks that integrate and synchronize the operations and activities of assigned COMCAM platoons.
- COMCAM equipment maintenance by on-site repair, replacement, or evacuation to civilian contractors.
- Liaison to supported units**,** joint COMCAM team, and other Service COMCAM elements.
- Establishment, operation and maintenance of COMCAM facilities required to support theater and subordinate tactical command posts.
- Operations and support facilities to provide tailored still and motion media products.
- Organizational maintenance of vehicles, power generators, environmental control units and signal support systems.
- Support of special operations forces (civil affairs, military information support operations, rangers and special operations aviation).
- Editing for the electronic processing of digital still and motion imagery acquired by organic documentation teams.
- Presentation and exploitation of visual imagery in support of operational requirements.
- Parachute landing capabilities (unique to airborne COMCAM company).

JOINT/AREA SIGNAL COMPANY

2-37. The joint/area signal company (JASC) is a key theater signal asset that provides engineers, installs, operates, maintains, and defends two large or medium command nodes plus four to ten extension command post nodes, the supporting LOS, BLOS assets, NM, cable and wire assets to provide garrison quality data services. The signal command (theater) ((SC(T)) employs the JASC throughout a theater of operation to extend U.S. communications systems and services to support deployed forces. It provides communications facilities in the theater for Army units from brigade to theater Army headquarters, ASCC commanders, combatant commanders, JTFs and joint forces land component commands throughout the execution unified land operations. This unit also provides the following capabilities to support the unit's mission—

- Automatic switching services for both analog and digital voice and data traffic, tactical multichannel high capacity transmission systems, and multichannel satellite ground terminals.
- Telephone switching services and Joint Network Node NetOps tools support NM within the company.
- Cable Teams for maintaining cable and wire systems.
- BLOS communication support in the form of SATCOM and tropospheric communications.
- Data services support and connectivity for the theater of operations and support of JTF missions.
- Petroleum, oil, and lubrication, vehicle recovery, field maintenance, and field feeding support for the company and headquarters and headquarters company when co-located.

EXPEDITIONARY SIGNAL COMPANY

2-38. The expeditionary signal company (ESC) provides synchronization of mission command warfighting function tasks, staff planning and supervision of an expeditionary signal company, consisting of headquarters element and two expeditionary signal platoons plus any augmenting elements, personnel or material assets.

2-39. The ESC provides communication facilities in the theater for Army units from brigade to theater Army headquarters, ASCC commanders, combatant commanders, JTFs and joint forces land component commands throughout the execution unified land operations. This unit also provides the following capabilities to support the unit's mission—

- Automatic switching services for both analog and digital voice and data traffic, tactical multichannel high capacity transmission systems, and multichannel satellite ground terminals.
- Telephone switching services and NetOps tools support NM within the company.
- Two cable teams for maintaining cable and wire systems.
- BLOS communication support in the form of SATCOM and tropospheric communications.
- Data services support and connectivity for the theater of operations and support of JTF missions.
- Petroleum, oil, and lubrication, vehicle recovery, field maintenance, and field feeding support for the company and headquarters and headquarters company when co-located.
- Company headquarters provides limited personnel services and logistical support of the company, which includes unit administration for assigned or attached elements, supply support, chemical, biological, radiological, nuclear, and high yield explosives support, and weapons support.
- Network management, field feeding support, field maintenance support on all organic communications-electronics and COMSEC equipment, and field maintenance on all organic automotive, power generation, and environmental control equipment. This support accommodates entire company deployments and when separate teams provide autonomous contingency communications packages.
- Multichannel teams provide range extension capability to support LOS and BLOS signal assets for an ESB.

EXPEDITIONARY SIGNAL BATTALION

2-40. The expeditionary signal battalion HQ provides mission command, administrative, and logistical support for an ESB. The HQs oversees the engineering, installing, operating, maintaining, and defending of nodal and extension communications in support of Army units, combatant commanders, ASCC, or joint force land component commanders. It also provides NM for all tactical communications assets within the battalion through the suite of NetOps tools.

2-41. The ESB engineers, installs, operates, maintains, and defends the network for various CPs. It provides voice, data, VTC, and special circuits over robust LOS and BLOS transmission systems (tropospheric, tactical satellite, and microwave) via an internet protocol based system, which allows for support of a greater number of subscribers. This unit also provides the following capabilities to support the unit's mission—

- Staff planning and supervision of the battalion and any attached units.
- NM of all tactical communication assets within the battalion.
- Maintenance of the unit property book for the battalion.
- Personnel and administrative services, logistical and religious support for assigned and attached units.
- Field feeding augmentation to the senior signal unit in the theater.
- Field maintenance support for the headquarters and headquarters company.
- Management of the COMSEC account for the battalion.
- Performs field maintenance on all organic equipment, and organic communications-electronics and COMSEC equipment.

THEATER TACTICAL SIGNAL BRIGADE

2-42. The theater tactical signal brigade conducts mission command for assigned and attached units. The HQs supervises the installation, operation, and maintenance of communications signal nodes, and engineers and defends these nodes, in the theater communications system, excluding the division and corps systems. It provides theater-level planning and engineering for mission command networks and systems, and baseline services. It also supervises the installation, operation, and maintenance of nodal communications in support of the Theater Army, coalition, and augmentation to the corps, division, other government agencies and non-government organizations. This unit provides the following capabilities—

- Planning, engineering, and control of the theater communications system.
- Coordination of the training, administration, and logistical support of assigned units.
- Allocates, controls, and positions available tactical network resources.
- Oversees connection of the network to Army, joint, interagency, and coalition forces.
- Ensures physical security and active defense of network resources.
- Performs long-range planning for tactical network expansion and upgrade.
- Enforces enterprise technical standards for all tactical network resources.
- Conducts system and network management.
- Provides oversight of contractor support operations/personnel.
- Provides training and readiness oversight and administrative and logistical support of multiple assigned signal organizations.
- Based theater operational requirements, may have responsibility for the total network environment in the assigned theater/area of operations. This includes assigned SSBs and related network enterprise center (NEC) operational functions and support.

REQUESTING SIGNAL SUPPORT

2-43. A requesting unit's G-6/S-6 is responsible to determine what signal support is required for the current mission based on information contained in the operations order. Signal support is not static and changes as the mission and circumstances change. The ASCC G-6, who is also the senior signal commander of a SC(T) except in CONUS, tasks Signal assets to support the requesting unit.

2-44. When tasked to a division, the requesting unit's G-6/S-6, in conjunction with their G-3/S-3, coordinates through the division G-6 to the ASCC G-6 to determine the extent of the support required. Any unit not tasked to a division should coordinate directly with the ASCC G-6 to determine provided signal support.

2-45. The Signal proponent develops organizational structures to support units requiring pooled signal assets, like the ESB. Upon receipt of orders, the supporting signal asset receives a change to their current command relationship to the supported command. The requesting command may be responsible to support these elements with sustainment capabilities (logistics, personnel services, and health service support).

2-46. When the operation order identifies the supporting signal unit, the requesting S-6/G-6 contacts that unit for coordination. The supporting signal unit provides connection to LandWarNet, and is not responsible for computers, telephones or any local area support.

2-47. The requesting unit should describe—

- The unit needing service and the number of connections for each service required.
- The services needed (NIPRNET, SIPRNET, voice, special circuits, and COMSEC key support).
- The DTG for required services.
- The location for required services.
- The supported unit battle rhythm for communications services.

SECTION III – SIGNAL ENABLING COMMANDS AND STAFFS

2-48. The signal enabling commands and staffs provide the NetOps and network transport for mission command information systems. These commands establish policy and guidance, execute NetOps, provide network transport, and defend LandWarNet. Through policy and transport, these commands maintain LandWarNet and the Army's ability to operate within the cyberspace domain. The following section describes their roles and responsibilities within the overall support architecture.

U.S. ARMY SIGNAL CENTER OF EXCELLENCE

2-49. The Signal Center of Excellence (SIGCoE) is the Signal Corps and Signal Regiment headquarters and serves as the force modernization proponent for signal in accordance with AR 5-22. It develops doctrine, organization, training, materiel, leadership and education, personnel, facilities (DOTMLPF) requirements, determines the scope of future capabilities development efforts, and determines integration tasks for both Army and joint operations under the oversight and guidance of the Chief Information Officer/G-6 (CIO/G-6), within TRADOC in accordance with AR 5-22. The SIGCoE integrates approved IA tools, doctrine, procedures, legalities, and techniques into applicable programs of instruction for TRADOC schools. They develop, test, and recommend operational and organizational concepts and doctrine to achieve IA goals and ensure compliance in accordance with AR 381-11.

THE SIGNAL CORPS AND REGIMENT

2-50. The Signal Corps is the compilation of all Signal Soldiers, which includes all Signal branch officers and warrant officers, and Signal career management field enlisted Soldiers. Soldiers become part of the Signal Corps and affiliate with the Signal Regiment (in accordance with AR 600-82). The Signal Regiment is the compilation of Signal Soldiers that affiliate with the Signal Regiment upon the completion of branch or military occupational specialty qualifying schools and the functional area officers that choose to regimentally affiliate. The SIGCoE is the Signal Corps and Signal Regimental headquarters.

THE SIGNAL PROPONENT

2-51. The SIGCoE is responsible for the execution of training, leader development, education, personnel lifecycle management functions and signal force modernization. The signal proponent is responsible for training all Soldiers, including officer, warrant officer and enlisted Soldiers, initially accessed into the signal career management field and branch designations. This responsibility includes training Soldiers that transition to signal military occupational specialty, functional areas (regardless of branch) and career field designations. The transition of Soldiers from other disciplines into the signal profession is necessary to meet the Army's requirement for Soldiers at the experience levels necessary for technically advanced training in unique skill sets required to operate and defend the network. Signal Soldiers receive training to—

- Plan and direct signal support to operations.
- Provide (engineer/install) network transport and information services (to include mission command system integration).
- Operate (restore, configure, allocate, optimize, and secure) telecommunications networks.
- Protect and defend the confidentiality, integrity, and availability of telecommunications networks, computer systems, and residing information.
- Conduct spectrum management operations.
- Conduct COMSEC.
- Conduct visual information operations.

2-52. The signal force modernization proponent is responsible for DOTMLPF requirements for all NetOps, network transport and information services, spectrum management operations, and visual information functions. The SIGCoE executes force management responsibilities, consisting of requirements definition, force development, capabilities development, doctrine development, training development, material development, leadership development and education, personnel development, facilities development, and policy relative to the Signal Corps. SIGCoE ensures its DOTMLPF actions are coordinated with Army commands, Army Service component commands, direct reporting units, field operating agencies, the Headquarters, Department of the Army staff, and others as required.

2-53. The SIGCoE integrates joint communication requirements during capabilities development to ensure the continued ability to network during joint operations. The joint capability areas provide a common lexicon for all services to use for multi-service capability development and operational planning. The joint capability areas are the collections of like DOD capabilities functionally grouped to support capability analysis, strategy development, investment decisionmaking, capability portfolio management, and capabilities-based force development and operational planning.

2-54. The Signal Corps integrates the joint capability areas to meet the requirements our Army and joint communications networks must provide to commanders at all levels. Signal Regiment personnel directly support the net-centric operations, joint capability area, providing communications that enable the other joint capability areas by extending the voice and data capabilities to the joint partners. The two joint capability areas that benefit most from this enhancement are command and control and battle space awareness, although all, force support, force application, logistics, protection, building partnerships and corporate management and support, also rely on the network during the execution of those capabilities.

Note. Refer to the Joint Electronic Library online, www.dtic.mil/futurejointwarfare/jca.htm for more information.

U.S. ARMY CHIEF INFORMATION OFFICER/G-6

2-55. The CIO/G-6 is the principle staff assistant and advisor to the Secretary of the Army on Army information management to include the strategy, policy, and execution of information management and information technology for the Army and the effects of information management and information technology on the warfighting capabilities. The CIO/G-6 provides guidance and policy on information technology systems and networks, to include reviewing and evaluating existing Army information management and information technology policies to determine their adequacy and oversee the implementation of policy and guidance. The CIO/G-6 sets the strategic direction for and supervises the execution of Army policy and programs for information management, including creating network architecture and information sharing policy, modernizing Army resource management processes and ensuring the synchronization of the Army’s network activities. The CIO/G-6 is also responsible for ensuring the execution of the Army Signal G-6 function, including providing the Secretary of the Army and Chief of Staff of the Army with advice on the effects of information management, information technology, and communications. The CIO/G6 is the principal official within Headquarters, Department of the Army with oversight responsibilities for all information technology resources under the provisions of the Clinger-Cohen Act. The CIO/G-6 performs the duties and responsibilities as assigned in AR 25-1 while executing the directorate’s mission.

ARMY CYBER COMMAND/SECOND U.S. ARMY

2-56. U.S. Army Cyber Command plans, coordinates, integrates, synchronizes and defends all Army networks. When directed, U.S. Army Cyber Command conducts cyberspace operations in support of unified land operations to ensure U.S. and unified action partner freedom of action in cyberspace, and denies the same to our enemies and adversaries. U.S. Army Cyber Command also serves as the ASCC under U.S. Cyber Command and provides reporting and situational understanding of LandWarNet. U.S. Army Cyber Command is the command and control authority for all collateral top secret and below Army NetOps. It is the single authority for the operation, management, and defense of LandWarNet global enterprise network. U.S. Army Cyber Command oversees and reports threats to the Army global enterprise network and, as required, other DOD agencies and their enabling technologies. In coordination with the CIO/G-6, supports information security and information assurance compliance for collateral top secret and below networks and systems. U.S. Army Cyber Command performs the duties and responsibilities as assigned in AR 25-1 while executing the commands mission.

U.S. ARMY NETWORK ENTERPRISE TECHNOLOGY COMMAND

2-57. The U.S. Army Network Enterprise Technology Command (NETCOM) plans, engineers, installs, integrates, protects, defends and operates LandWarNet, enabling mission command through all phases of unified actions. NETCOM's task is to be the Army's global network enterprise service provider, executing cyberspace operations on behalf of U.S. Army Cyber Command and attaining information superiority, achieving a joint, interagency and multinational network enterprise.

2-58. NETCOM serves as the designated approval authority for the Army enterprise, as directed by the CIO/G-6. NETCOM serves as the Army information technology integrator to achieve a single, virtual enterprise network by advising the end-to-end management of the Army's enterprise service area, which includes service delivery, service operations, and infrastructure management. NETCOM prescribes all service delivery activities, policies, processes, procedures, and protocols for configuration management, availability management, capacity management, change management, and release management for the Army's networks and functional processing centers.

2-59. NETCOM is responsible for managing the Army's LandWarNet to include establishing the networthiness, IA, technical and configuration management programs and policies in accordance with AR 25-1 and AR 25-2. NETCOM manages the administration of amateur radio operations and the Army Military Auxiliary Radio System program per AR 25-6 and provides COMCAM documentation support for Theater Army and joint military operations unified land operations. They are the single entry point to submit validated, approved telecommunications requirements to Defense Information Systems Agency (DISA) for coordination and implementation. NETCOM performs the duties and responsibilities as assigned in AR 25-1 while executing the commands mission.

NETCOM G-33

2-60. The NETCOM G-33 serves a dual role, both the NETCOM G-33 and under operational control of U.S. Army Cyber Command. Operations are exercised through the Army Cyber Operations and Integration Center. The NETCOM G-33 mission is to assist U.S. Army Cyber Command in providing Army and DOD NetOps reporting and situational understanding for LandWarNet across the strategic, operational, and tactical levels. The Army Cyber Operations and Integration Center maintains operational control of all Army Theater Network Operations and Security Centers (TNOSCs) and Regional Network Operations and Security Centers (RNOSCs). The G-33 exercises the following functions—

- Directs the mission command of the full spectrum of cyberspace operations (DOD information network operations, defensive cyberspace operations, and offensive cyberspace operations).
- Direct, manage and enforce NetOps policies, orders and directives as well as report compliance.
- Collaborate with the NetOps community to ensure effective operation and defense of LandWarNet.
- Provide NetOps situational awareness and reporting for LandWarNet.
- Serve as the single inject point for Army NetOps to U.S. Cyber Command.
- Coordinate and direct network troubleshooting and restoral actions.
- Support the coordination, synchronization and direction of actions in response to CND incidents.
- Monitor and report compliance with issued orders and directives.
- Execute activities, methods, procedures, and employ NetOps capabilities enabling operation, administration, maintenance and provisioning of managed network resources.
- Review, monitor, assess, and recommend approvals for major enterprise infrastructure initiatives, such as, integration, requirements analysis, lifecycle development, configuration management and performance management of information systems across LandWarNet.
- Ensure process compliance and infrastructure requirements are compatible with all required DOD and Army standards and regulations.

2-61. Maintain oversight of all LandWarNet information technology assets, including gathering system requirements, establishing baselines and incorporating processes to ensure continued readiness and availability.

U. S. ARMY SPACE AND MISSILE DEFENSE COMMAND

2-62. The U.S. Army Space and Missile Defense Command/Army Forces Strategic Command G-6 is designated as the Wideband SATCOM System Expert, the Consolidated Narrowband SATCOM System Expert, the Wideband Global SATCOM System Expert, the Defense Satellite Communication System SATCOM System Expert, the Global Broadcast Service SATCOM System Expert and the Mobile User Objective System SATCOM System Expert responsible for engineering, operating, and the technical expertise of its assigned satellite systems. U.S. Strategic Command assigned operational control of the four Regional SATCOM Service Centers to the U.S. Army Space and Missile Defense Command/Army Forces Strategic Command.

2-63. The regional SATCOM support centers operate around the clock to provide SATCOM resources, systems engineering, and modeling support for decision makers, national activities and agencies, and other SATCOM users. The regional SATCOM support centers analyze requirements and develop solutions to support assigned users in day-to-day management of SATCOM resources allocated for the combatant command. This includes execution and implementation of the combatant commands directed assignments to subordinate and geographically associated organizations. They also process the satellite access request portion of valid two-part satellite/gateway access requests to authorize access to, and the use of, space and ground terminal resources via the satellite access authorization.

SIGNAL COMMAND (THEATER)

2-64. The SC(T) provides oversight, leadership and direction over theater signal organizations that are either service assigned to or in direct support of the signal command. These theater signal organizations can include deployable formations such as theater tactical signal brigades(s) with their associated expeditionary signal battalions (ESBs), combat camera assets, and inside/outside plant capability in the form of tactical installation and networking (TIN) companies. Non-deploying structures include theater strategic signal brigades (TSSBs) with their associated NEC (CONUS) or strategic signal battalions (OCONUS), fixed satellite communications facilities, and a host of other strategic capabilities. Though non-deploying by design, these organizations can, based on mission requirements, deploy personnel with specific technical skill to support ongoing operations.

2-65. The SC(T) executes mission command for assigned and attached units to provide NetOps, in support of Army, joint, multinational and interagency missions. It functions at the corps/Army and theater headquarters level to provide NetOps and SMO support to the theater, joint, multinational forces. The SC(T) provides the following capabilities to support the command's mission—

- Mission command/administrative functions for all assigned or attached units as directed.
- Delivery of common user services in support of combatant commanders.
- Planning and coordinating corps signal reserve component training.
- The SC(T) Commander may also serve as the Army Service component command G-6 (ASCC G-6).
- Property book services for its organizational elements.
- Plan, engineer, and manage signal support systems installed by the SC(T) and network interfaces to existing systems installed by joint, multinational units.
- Plan, engineer, integrate and rehearse LandWarNet information systems and networks, to include capital planning; ensure LandWarNet capabilities are prioritized and available as a capability to senior mission commanders.
- Provide operational management of signal assets responsible for install, operate, maintain and defend theater LandWarNet.
- Plan, engineer, and manage requirements for special purpose information systems.

- Execute theater NetOps; improve Army's ability to adjust network priorities, global availability, and to enforce policies and standards within the joint NetOps framework.
- Organic engineering capability used to support systems design and policy development and implement capabilities needed to support theater NetOps.

THEATER STRATEGIC SIGNAL BRIGADE

2-66. The mission of a theater strategic signal brigade is to provide operational base and sustaining signal support (long-haul and tactical communications, automation, and network management) to maintain the warfighter in an area of responsibility and to enable power projection platforms required for force projection.

2-67. These units provide the following—

- Executes mission command over strategic signal battalions and assigned units.
- Installation, operation and maintenance of tactical interface, and sustaining base and strategic signal support functions (communications, automation, and network management) to sustain the warfighter in an area of responsibility.
- NetOps at the installation level.
- Within CONUS, provides operational direction to the NEC in the provisioning of C4IM services.
- Access to LandWarNet for all Army assets assigned to a geographic area and to tactical Army assets deployed in other theaters.
- Advice to the commanders, staff, and information system users on the capabilities, limitations, and employment of all tactical and non-tactical signal and network assets available to a particular supported command.
- Advice to the supported commanders and staff on IM, automation policy, technical matters, performance, and supervision of system analysis and programming functions on related abilities.
- Input pertaining to enemy capabilities, intention and vulnerabilities regarding the DODIN and LandWarNet to all-source intelligence assessments and estimates at the operational and strategic levels. This also entails predicting the enemy courses of action, producing threat estimates, ensuring proper dissemination of intelligence information and products, and evaluating intelligence products as they relate to LandWarNet and the DODIN.

STRATEGIC SIGNAL BATTALION

2-68. The strategic signal battalion (SSB) provides synchronization of mission command warfighting function tasks of the operations and activities of assigned communications and signal support teams/units. The headquarters detachment provides unit administrative and logistical support to assigned personnel.

2-69. SSBs are regionally based signal elements with varying quantities of support teams assigned, equipment and information mission requirements. They manage communications facilities and infrastructure in their respective regions, and are responsible for installing, operating, maintaining, and defending network facilities in support of theater strategic signal brigade, SC(T) and NETCOM missions. Some of its assigned subordinate elements may operate and maintain equipment at static locations or fixed sites. The SSB provides the following common capabilities to support the unit's mission—

- Staff planning and operational supervision of assigned teams.
- Supervision of the functions of signal support, communications, automation, and visual information.
- Planning, engineering and control of strategic communications systems.
- Coordination of the administration, vehicle maintenance, religious, and logistical support to assigned units.

2-70. SSBs and their companies provide the following capabilities to satisfy specific regional signal support requirements based upon the supported command's mission—

- Planning, operations, coordination, and management of the supported unit's telecommunications systems and information systems support functions for mission command.
- Spectrum planning and management.
- Coordination and direction of information processing systems, to include data system studies and preparation of documentation and specifications for proposals.
- Oversight of the installation, operation, and maintenance of electronic switches and NetOps equipment, radio receivers and transmitters, and other associated equipment.
- COMSEC material issue and management.
- Installation, operation, and maintenance on multi-functional/multi-user information processing systems, including peripheral equipment and auxiliary devices.
- Planning, requirements analysis, design, development, testing, installation, maintenance and training for all automation data processing systems.
- Installation and maintenance of copper and fiber optic cable systems, repeaters, restorers, voltage protection devices, telephones, distribution frames and related equipment.
- Installation and removal of wire systems, including telephones.
- Voice and data switching, routing and multiplexing coupled with COMSEC devices, to provide a shelter-based mobile voice and data switching upgrade to existing tactical communications.
- Network connectivity to include NIPRNET, SIPRNET, DRSN, DSN, and related private branch exchange services and video teleconferencing.
- Satellite access using military constellations or commercial satellites operating in the super high frequency and extremely high frequency ranges (C, X, L, Ku and Ka bands).
- Ensuring all systems have a certificate of networthiness.

Note. The SSBs execute the NEC missions for Army posts, camps, and stations in OCONUS.

NETWORK ENTERPRISE CENTER

2-71. The NEC provides overall NetOps for the data and voice networks and is the designated information manager and information technology manager on their post, camp, or station (or within an assigned geographical area). NECs plan and budget for appropriate network and information systems hardware and software technology upgrades or replacements, to meet customers' validated requirements. NECs work with external organizations to ensure the proper operation of installation-level components of DOD or Army-level networks and information systems. The NEC NetOps responsibilities include—

- Managing all support functions associated with providing customer access to the installation common-user networks and information systems infrastructure.
- Ensuring support and problem resolution for physical networks and information systems equipment on the installation or within the NEC's direct area of operations.
- Representing their supported units in recommending changes to LandWarNet based upon lessons learned and innovative ideas.
- Implementing NetOps practices in accordance with DOD, Army, and SC(T) policy and guidance.
- Establishing policies and procedures for the performance of the operation and maintenance of networks and information systems within its AO.
- Establishing individualized service level support agreements between installation/post/camp/station tenants and the SC(T), and coordinating with the SSB for management of inter-installation networks and information systems that affect their supported organizations.
- Establishing and managing the command IA program for post/camp/station.
- Managing the activities, functions, and capabilities of the network and information systems resources within its region in accordance with direction from the SC(T) and TNOSC.
- Providing mission impact of outages, CND incidents, and other network issues to the TNOSC and SSB operations center.

REGIONAL NETWORK OPERATIONS AND SECURITY CENTER

2-72. The Regional Network Operations and Security Center (RNOSC) provide NM and information dissemination management (IDM) services to augment its assigned strategic signal battalion.

2-73. The RNOSC is regionally located at fixed station sites in assigned theaters and provides direct support NM and IDM assistance to the supported strategic signal battalion. The TNOSC maintains oversight of the RNOSC and provides NetOps directives. The RNOSC inherits the DOD Information Assurance Certification and Accreditation Process, vulnerabilities, and threats of the TNOSC. This unit also provides the following capabilities to support the unit's mission—

- Operation and maintenance management of the RNOSC with command, control, communications, computers and information management support for network systems.
- Operations and maintenance data systems administration with reports on security intrusions.
- Personnel network status reports on circuit outages to the Army Cyber Operations and Integration Center and TNOSC.
- IA (monitoring networks, relaying information, and security procedures).
- Status reports on security procedures for all major systems within the command.

SIGNAL CENTER/THEATER NETWORK OPERATIONS AND SECURITY CENTERS

2-74. Assigned to the SC(T), under OPCON to U.S. Army Cyber Command's Army Cyber Operations and Integration Center, the TNOSC mission is to act as the single point of contact for Army network services, operational status, and anomalies in the theater. The TNOSC provides visibility and status information to the U.S. Army Cyber Command's Army Cyber Operations and Integration Center. In some theaters, the TNOSC may provide visibility to other Service component NOSCs. There are six TNOSCs established for all theaters of operations: CONUS (CONUS and South), Europe, Pacific, Korea, and Southwest Asia. The TNOSC functions are interchangeable across all theaters. NetOps personnel can perform theater common functions at multiple geographical locations and should perform them the same way at each location.

2-75. The TNOSC performs or coordinates any task that spans the theater or multiple regions. This provides consistent service among regions. It also places the operational function at the only location in the enterprise that would have visibility or awareness of what was happening in both regions. Security, operation, and maintenance of the specific theater LandWarNet infrastructure are the exclusive responsibility of the TNOSC. The TNOSC is responsible for providing LandWarNet theater enterprise services to the NECs. Each TNOSC is also responsible for ensuring Army information systems providing these services are configured and maintained according to—

- Applicable Defense Information Security Agency's Security Technical Implementation Guides.
- Army best business practices.
- Best security practices.
- Vendor and industry guidance as directed by NSA security readiness guides.
- Chairman Joint Chiefs of Staff Manual (CJCSM) 6510.01B.
- Department of Defense Instruction (DODI) 8500.2 and AR 25-2.

2-76. Each theater has a Regional Computer Emergency Response Team which provides the following—

- Conduct threat based vulnerability assessments and defensive cyberspace operations-response actions and mitigation countermeasures development and strategies.
- Conduct signature attack sensing and warning analysis. Develop mitigation strategies to support network defense requirements and data loss prevention, including spillage.
- Incident handling and incident response actions in accordance with AR 25-2, DOD O-8530.1-M and CJCSM 6510.01B.
- Conduct computer defense assistance program (penetration testing, network assistance visits, and network damage assessments) in support of the mission commander and subordinate theater units.

Chapter 3

LandWarNet

The Army is transitioning from the philosophy of connecting secure network autonomous enclaves in the different theaters to an interdependent security posture operating as a system of systems. LandWarNet is a mission command enabler, and the Army's portion of the DODIN upon which both the generating force and the operational Army depend on throughout all phases of operations and operational environments. This chapter discusses the DODIN and LandWarNet, the network transport and information services capabilities that enable mission command, NetOps, and cyber threats. Some communications organizations within DOD refer to LandWarNet as the "Army enterprise network." This publication uses LandWarNet as the doctrinal term for the Army's portion of the DODIN.

SECTION I – THE DEPARTMENT OF DEFENSE INFORMATION NETWORKS AND LANDWARNET

THE DEPARTMENT OF DEFENSE INFORMATION NETWORKS

3-1. The *Department of Defense information networks* consist of the globally interconnected, end-to-end set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems.(JP 1-02). The DODIN is the worldwide network made up of LandWarNet integrated with the other Services' networks.

3-2. The DODIN is part of cyberspace. The emergence and use of cyberspace as an operational domain influences signal support to military commanders. The DODIN, as a part of cyberspace, interacts with and provides connections to national and global cyberspace, the national information infrastructure, and global information infrastructure, respectively. The DODIN encompasses capabilities provided by the Army LandWarNet, the Navy FORCEnet, and the Air Force C2 Constellation Network, as shown in Figure 3-1 on page 3-2.

3-3. The DODIN is capable of storing users' data or making data stores available in other cloud computing environments. Authorities manage the applications and services, which reside within the DODIN. Data centers exist in every GCC's area of responsibility. These processing nodes are essentially stacks of servers, with the fundamental purpose of 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 their data from their current (home station) data center to the data centers in the theater of operations. Data centers support a worldwide DOD intranet by which a single connection allows a user to access Army, joint and coalition data, applications and information services from anywhere, at any time, in any network environment.

- **Cloud Computing** is a mode of architecture 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. DISA is the DOD enterprise cloud service broker. As the enterprise cloud service broker, DISA is responsible for making it easier, safer, and more productive to navigate, integrate, consume, extend, and maintain cloud services within the DOD, and with other Federal and commercial cloud service providers. DOD components acquire cloud services by using the broker, or obtain a waiver from the DOD CIO designated review authority.

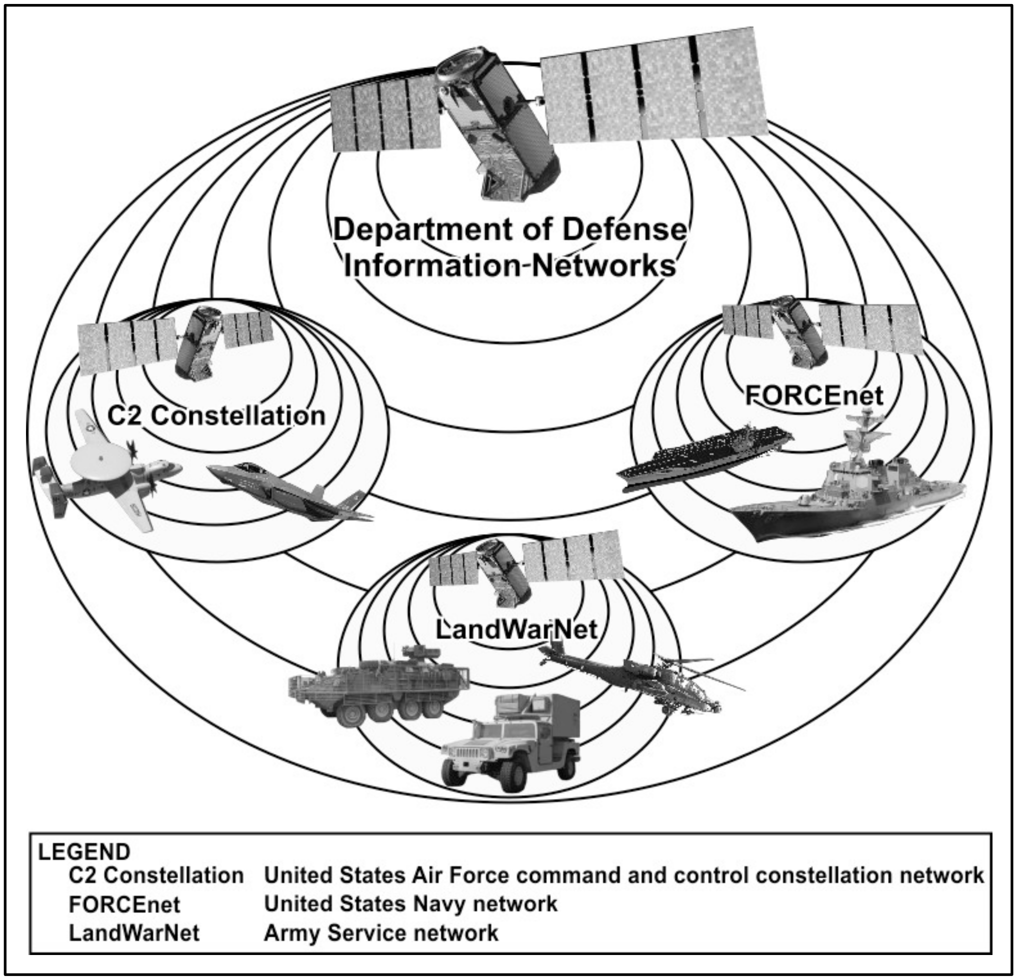

Department of Defense Information Networks
C2 Constellation
FORCEnet
LandWarNet
LEGEND
C2 Constellation United States Air Force command and control constellation network
FORCEnet United States Navy network
LandWarNet Army Service network

Figure 3-1. The Department of Defense information networks

- **Satellite Transport** includes all DOD satellite communications (data and voice). Satellite communications, such as Wideband Global SATCOM and DOD Gateway, extend the DODIN to users without fiber connections, providing improved connectivity and data transfer capability.
- **DISN** includes any DOD system, equipment, software, or service that transmits, stores, or processes DOD information, and any other associated services necessary to achieve information advantage. DISN services include SIPRNET, NIPRNET, Joint Worldwide Intelligence Communications System, VTC, DSN, DRSN, Defense Research Engineering Network, and global mission network. The three segments of DISN include the sustaining base, long-haul and deployed. The long-haul segment connects the sustaining base to the deployed portion of the network.

3-4. The Joint Information Environment (JIE) is a secure environment that shares information technology infrastructure, enterprise services and a single security architecture within DODIN. The JIE achieves full spectrum superiority, improves mission effectiveness, increases security and realizes information technology efficiencies. The JIE operates per the unified command plan using enforceable standards, specifications, and common tactics, techniques and procedures. JIE improves operational effectiveness, standardizing training and equip requirements across combatant commands and geographic regions, enhancing security and allowing Services and agencies to better reallocate and align existing resources.

LANDWARNET

3-5. LandWarNet is the Army's contribution to the DODIN and JIE. LandWarNet is a single, secure, standards-based, versatile infrastructure nested within the DODIN. It is linked by networked, redundant transport systems, sensors, warfighting and business applications, and services. LandWarNet provides Soldiers and civilians timely and accurate information in any environment to enable decisive action with our unified action partners.

3-6. Just as DODIN is the DOD's application of cyberspace, LandWarNet provides the Army access to the cyberspace domain. LandWarNet contains network service centers (NSCs) in a cloud computing environment connected with long-haul network transport, and supports the following—

- Installation campus transport networks for known, verified users. Campus networks connect installation-based users to an area processing center and DISN services.
- Regional hub nodes that provide transport capabilities for deployed users and training environments to virtually link deployed forces to area processing centers. The hub node is a LandWarNet satellite transport component that extends DISN services to Army deployed forces.
- Tactical internet networks to connect deployed users to an area processing center and other DISN services, regardless of their location. Tactical networks connect to LandWarNet and the DODIN through the regional hub nodes.
- Lower tactical internet network infrastructure to support maneuver units to execute decisive action missions.

3-7. LandWarNet greatly enhances the potential for network integration, and provides a powerful tool for leaders to use in synchronizing their efforts. LandWarNet also allows subordinate and adjacent units to use their common understanding of an operational environment and commander's intent to synchronize their actions with those of other units without direct control from the higher headquarters.

LANDWARNET ARCHITECTURE

3-8. LandWarNet architecture is a cloud-computing environment that provides access to protected services at the point of need. LandWarNet operational view (Figure 3-2 on page 3-4) shows LandWarNet as an enterprise information environment that optimizes the use of Army IT assets to converge communications, computing, and enterprise services into a single joint platform that commanders can leverage for all missions.

3-9. LandWarNet provides protected services for cloud computing through a defense in depth posture, and data stores from within the same network cloud. Security is critical, at the forefront of cloud computing, and focuses on the security of critical information.

3-10. The logical boundary between LandWarNet and the rest of the DODIN is the Army security boundary, known as the top-level architecture. The top-level architecture consists of firewalls, intrusion detection, and intrusion protection sensors. Each SC(T) has multiple top-level architectures within their respective area of operations providing redundant, seamless connections to the DODIN. The hardened outer perimeter of the top-level architecture controls access to vital applications and data within LandWarNet. The DODIN inherits the threats through connections from the most vulnerable communications assets within the computing environments.

3-11. The Signal Corps' core competencies enable LandWarNet's seamless cloud environment through—

- The core competency of network transport and information services provides the network cloud with its applications and services.
- The core competency of NetOps and its essential capability of COMSEC secure the network and ensure access to the cloud.

3-12. The core competency of SMO enables LandWarNet systems that rely on wireless connectivity to perform their functions in the intended environment without causing or suffering unacceptable frequency fratricide.

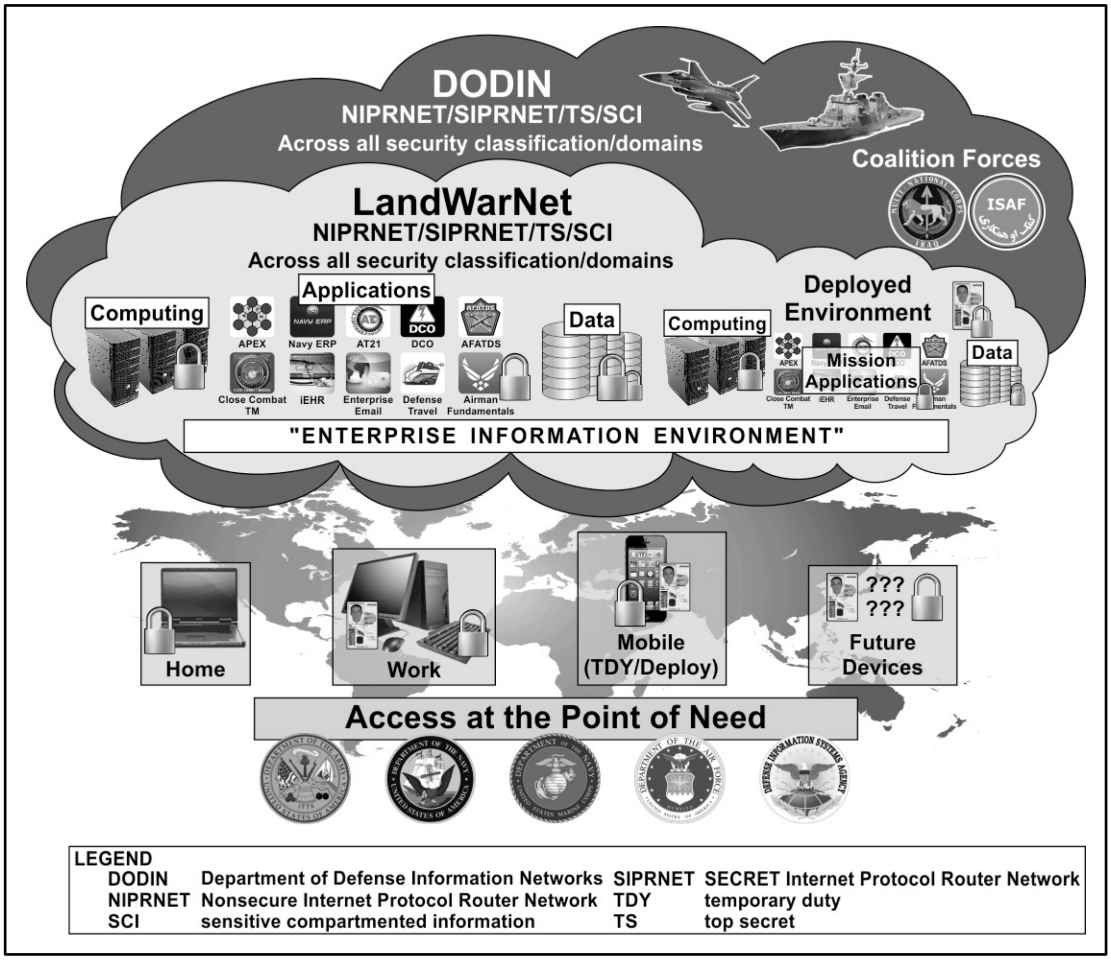


Figure 3-2. LandWarNet operational view

LandWarNet Operating Environments

3-13. Work, deployed, home, and mobile represent LandWarNet's different operating environments. The standards-based approach to LandWarNet NetOps allows all of these environments to operate as a single, integrated network cloud. LandWarNet operational view (Figure 3-2) depicts a visualization of how members of the U.S. Army in each of these environments access protected data and services through the cloud.

Work Environment

3-14. Generating forces occupy posts, camps, and stations throughout CONUS and OCONUS in support of GCCs. The work environment is the Army-in-garrison, using LandWarNet as a strategic capability.

3-15. NECs are network service providers to installations. The paradigm has shifted away from locally provided services to an enterprise approach that makes global operation and defense of the Army's network possible. The NEC manages the installation campus area network, and ensures agreed-upon service levels for the supported units at work in garrison. The installation campus area network connects installation-based users to the DISN, secure data stores, and baseline common services found in the Command, Control, Communications, Computers and Information Management (C4IM) Services List. Net-centric enterprise services are the joint standard. The information services the NEC provides in CONUS are the same information services the strategic signal battalions provide OCONUS. LandWarNet provides the following baseline services as outlined in the C4IM Services List—

- Communications systems and system support services (Service 15).
  - Telephone and data infrastructure services.
  - Emergency communications telephone services.
  - Wireless infrastructure services.
  - VTC services.
  - Range/field telephone services.
  - Telecommunications continuity of operations plan and operations plan support services.
  - Fire, safety, security, and other circuit services.
  - Non-tactical radios and tactical radio spectrum management services.
- Information assurance services (Service 18).
  - Defense in depth.
  - COMSEC services.
  - Risk management/accreditation/certification policy services.
  - Network security services.
- Automation Services (Service 19).
  - Mail messaging/collaboration (E-mail/defense messaging system) and storage services.
  - Desktop/software/peripheral support services.
  - Web support services.
  - Automation and network continuity of operations plan and operations plan support services.
  - Automation and network service support services.

3-16. Generating forces are transitioning to receiving their network connectivity and patches for their tactical systems directly from the local NEC. This process of using the installation as a docking station provides a standard, simplified connection for operating forces to connect their mission command systems to an installation's secure network. This allows active and reserve-component units who operate tactical information systems during exercises and deployments to train and work in garrison as they would during deployments.

3-17. Installation as a docking station provides consistent, streamlined and cost-effective connectivity at the garrison; enables administrators to keep user accounts current and systems patched to mitigate security threats; allows users access to the same information technology systems and software used on the battlefield, enabling the Army to train as we fight providing Soldiers the capability to train on the same warfighting application terminals used during deployment. A Soldier could be training at an Army installation in CONUS, receive an alert and an order to deploy elsewhere, and that Soldier is only required to pack that terminal and begin movement. Once the Soldier arrives at the destination, the Soldier connects right back to the DODIN. Installation as a docking station reduces the time required to establish a compliant deployed tactical network through an always-on concept. The installation as a docking station system physically resides at the garrison installation but is logically its own network environment. When deployed, the baseline compliancy variables are already inherent. The supporting signal team can then focus on threats and variables associated with the mission.

3-18. Soldiers access global mission networks through installation as a docking station. The mission network information stores are now available to Soldiers throughout the operations process. Installation as a docking station facilitates planning, preparing and continual assessing of operations on the same mission network used during the execution phase.

Deployed Environment

3-19. Deployed tactical forces connect to the cloud-computing environment via DISA long-haul, DOD Gateway, or a regional hub node. Under the Army’s modular force design, theater army units have limited signal/network support capability. These units include Army Service component commands, corps, divisions, brigade combat teams, and multifunctional support brigades.

3-20. The NOSC/network operations center, under the senior signal commander, centrally manages the forward-deployed installation campus area networks. The installation campus area network relies upon

DISA long-haul transport for LandWarNet availability and the tactical internet satellite transport to access cyberspace. The tactical internet provides connectivity through a series of converged (voice-data-imagery-video) capabilities to the tactical edge. Protection and defense of this capability occurs within cyberspace. The tactical internet enables aggregation of intelligence and information from Soldiers, platforms, and command posts. The satellite transport connects through regional hub nodes or the DISA managed DOD Gateway.

Home/Mobile Environments

3-21. A significant number of network users operate in the cloud from outside the essential governing parameters of the Army network. These are users accessing the network from home or from a temporary duty location. Unavoidably, this particular set of users access the network through the Internet. Users within the home/mobile environments access LandWarNet cloud through commercial telecommunications access to an Army or other Service network entry point.

3-22. The enterprise network is only as strong as its weakest connection. Assured compliance standards associated with a defense in depth security posture are the shared responsibility of the supported user and the supporting service provider. Access to data and application services depends upon compliance with the current network security posture.

SECTION II – NETWORK TRANSPORT AND INFORMATION SERVICES

3-23. Network transport and information services capabilities are essential in supporting all Army organizations in the conduct of unified land operations. Network transport and information services capabilities connect users, information systems, and applications at all echelons across the enterprise. Network transport and information services includes human interaction, application interoperability with the network, and interoperability with joint, coalition, and commercial capabilities. Network transport and information services capabilities enable mission command applications and commanders' critical information exchanges to get the right information to the right place at the right time in a format that meets the requirements of leaders and Soldiers while training at home station and through all phases of an operation.

3-24. Transport provides the highway to pass information between data systems, platforms, and sensors. Services provide basic and common computing and networking capabilities that support the functional application. Services allow the free flow of data and information among and between applications and systems. The goal is a common toolset of information technology infrastructure services.

NETWORK TRANSPORT

3-25. Network transport is a system of systems including the people, equipment, and facilities that provide end-to-end communications connectivity for network components. The system of systems and end-to-end communications connectivity relative to network transport enables network transport systems to transmit and receive voice, data and video enabling support of warfighting functions to unified land operations. Network transport and services capabilities are part of a multi-tiered construct that combines advanced communications and network management technologies with the expertise, skills, and capabilities of network professionals at theater army, corps, brigade, and battalion levels. The systems and people combine with globally positioned network transport and services capabilities that provide access to network services, to space communications assets, and to robust and responsive aerial and terrestrial communications layers, form the always-on global network that enables mission command in support of unified land operations.

3-26. The key transport for the work environment is the sustaining base and long-haul backbone communications provided by DISA as part of the DISN services within the DODIN (JP 6-0). Network transport encompasses the integrated space, aerial, and terrestrial capabilities that provide access for Soldier and sensors through joint and strategic levels. Network transport capabilities support information requirements. Key network transport capabilities for the operating force are—

- Servers, routers and switches, and other network infrastructure.

- Tactical radios.
- Satellite communications.

3-27. Satellites and tactical radios are the core transport and information networking capability that enables mission command in support of unified land operations. These communications transport capabilities are across all Army echelons, enabling unified land operations in an integrated LandWarNet environment. Transparent to the user, the network provides access via the most expeditious/available transport layer in accordance with requirements and established policies. Ensuring adequate transport capability is a critical prerequisite to reliance on cloud computing and a paradigm shift away from locally provided services to an enterprise approach.

INFORMATION SERVICES

3-28. Information services consist of—

- Messaging – enables warfighters to exchange information among users and systems utilizing the network. Messaging examples include email, unique message formats, message-oriented middleware, instant messaging, and alerts.
- Discovery – enables warfighters to discover information content or services that exploit unique descriptions stored in directories, registries, and catalogs. An example of a discovery service is a search engine.
- Mediation – enables system interoperability by processing data to translate, aggregate, fuse, or integrate it with other data.
- Collaboration – provides the ability for warfighters to work together and jointly use selected capabilities. Examples of collaboration services are chat, on-line meetings, and work group applications.
- Storage – provides the physical and virtual hosting of data on the network with varying degrees of persistence, such as archiving, continuity of operations, and content staging. Standing operating procedures or operations orders may list the storage locations of information in the unit.
- User Assistance – provides centralized, automated access to lessons learned information that reduces the effort required to perform work force intensive tasks.

3-29. Through a full suite of information services, commanders and Soldiers collect, process, store, transmit, display, and disseminate information, as well as share and collaborate with unified action partners through all phases of an operation anywhere in the world. Information sharing allows for the mutual use of information services or capabilities. This ability may cross functional or organizational boundaries. Global authentication, access control, and directory services facilitates information sharing, which allow any authorized user with common and portable identity credentials to have access to, and visibility of, all appropriate operational, business support, or intelligence related information, services, and applications related to their mission and communities of interest.

3-30. A networked force has the ability to expand its operational reach by allowing dispersed elements to use nonorganic information services of other organizations. By integrating information from across the breadth of the area of operations, Army forces are able to maintain more relevant and complete situational understanding. This integrated picture allows commanders to employ the right capabilities, in the right place, and at the right time. Achieving this capability is essential to enable unity of command.

SECTION III – NETWORK OPERATIONS

3-31. NetOps is the discipline within signal operations focused on planning, engineering, installing, operating, maintaining, controlling, and defending the network in support of both the generating force and the operational Army. The purpose of NetOps is to assure system and network availability, assure information protection, and assure information delivery, which protects and maintains freedom of action for DOD missions within cyberspace. Effective NetOps is the availability of service, which facilitates network-enabled operations. NetOps is a commander-focused activity. All NetOps activities and functions support operational commanders. An effective NetOps mission command structure provides unity of command and unity of effort.

DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS

3-32. NetOps functions are conducted to operate and defend the Department of Defense information networks. Visibility of NetOps across the DODIN is critical to situational understanding and decisionmaking. Shared situational understanding for all aspects of NetOps, along with coordination between stakeholders on potential events, ensures joint force commanders are aware of network actions taking place in their area of operations. Joint force commanders have final authority over network activities in their area of operations during contingency operations.

3-33. Each Service maintains a NOSC, and is required to provide NetOps support to the GCCs. The means of accomplishing the NOSC mission is at the discretion of the individual Services. The Army is the only Service that elected to establish separate NOSCs in each theater.

3-34. Department of Defense information network operations involves the employment of the following joint network operations tasks—

- Enterprise management. Enterprise management is the technology, processes, and policies necessary to effectively and efficiently engineer, install, operate, manage, administer, optimize, and restore communications networks, information systems, and/or applicable applications that comprise the DODIN. This essential component merges IT services with the NetOps critical capabilities.
- Network assurance. Network assurance is composed of IA, CND, and critical infrastructure protection. Network assurance provides true end-to-end, defense in depth protection that ensures data confidentiality, integrity, and availability, as well as protection against unauthorized access. Network assurance incorporates those actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks.
- Content management. Content management allows NetOps centers to optimize the flow and location of information over the DODIN by positioning and repositioning data and services to optimum locations on the DODIN in relation to the information producers, information consumers, and the mission requirements.

LANDWARNET NETWORK OPERATIONS

3-35. LandWarNet NetOps is an integrated construct of the Department of Defense information network operations critical tasks enterprise management, network assurance, and content management; situational understanding, and the mission command activities that guide signal entities in the installation, management, and protection of communications networks and information services necessary to support operational forces.

3-36. LandWarNet NetOps provides integrated network visibility and end-to-end management of networks, global applications, and services across LandWarNet. Network visibility enables commanders to manage their networks as they would other warfighting platforms. The NetOps mission is to operate and defend LandWarNet. Unlike many missions deemed successful at a defined completion date, the NetOps mission is perpetual, requiring continual support to be successful. The measurement of effectiveness of NetOps is in terms of availability and reliability of network enabled services, across all areas of interest, in adherence to agreed-upon service levels and policies. NetOps essential tasks integrate at the strategic, operational, and tactical levels and across all warfighting and business functions to be successful. The effects created by NetOps are system and network availability, information protection, and information delivery, which gain and maintain information advantage for Army and joint missions within cyberspace.

3-37. The Army's two core competencies, combined arms maneuver and wide area security, provide the means for balancing the application of the elements of combat power within tactical actions and tasks associated with offensive, defensive, and stability operations; whereas the Signal Corps' core competencies define its distinct, unique, and valuable contribution in support of mission command to unified land operations. NetOps as a core competency of the Signal Corps has three essential tasks. The three essential tasks are—

- Provide NM/Enterprise Systems Management (ESM) – Engineer, install, operate, manage, maintain, and restore LandWarNet communication and computer networks, systems, and applications to achieve information advantage in support of unified land operations. NM provides networked system services with the desired level of quality and guaranteed availability. ESM comprises all measures necessary to ensure effective and efficient operation of information systems, elements of systems, and services. ESM provides day-to-day management of information systems, elements of systems, and services to include operating systems, databases, and hosts of the end-users. The NM/ESM function of LandWarNet NetOps corresponds to, and nests within, the function of enterprise management.
- Perform IA/CND – Protect and defend communications and computer networks, systems, and information services to deny unauthorized access and disruption of service. IA measures protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. IA includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. *Computer network defense* measures protect, monitor, analyze, detect, and respond to unauthorized activity with Department of Defense information systems and computer networks (JP 6-0). CND measures also defend networks, information, and computers from disruption, denial, degradation, or destruction. CND response actions execute authorized defensive measures or activities that protect and defend systems and networks under attack or targeted for attack by adversary computer systems/networks. COMSEC capabilities protect information transiting terminal devices and transmission media from adversary exploitation. The task of IA/CND corresponds to, and nests within, the function of network assurance and the passive measures in defensive cyberspace operations.
- Perform IDM/content staging (CS) – Emplace, manage, provide, and restore information services to enable information management/knowledge management (KM) and decision superiority. IDM/CS consists of the technologies, techniques, processes, policies, and procedures necessary to provide warfighters technical awareness of relevant, accurate information; automated access to newly revealed or recurring information; and timely, efficient and assured technical delivery of information in a usable format. IDM enables warfighters to perform network-enabled information management tasks and seeks to achieve the dissemination of the right information, to the right place, at the right time, and in a usable format. CS is a technique by which information is compiled, cataloged, and cached. The task of IDM/CS corresponds to, and nests within, the function of content management.

3-38. NetOps pertaining to corps, divisions, brigade combat teams, and maneuver battalions are not applied to the entire LandWarNet. Thus, the critical tasks listed above are at the operational and tactical levels.

3-39. LandWarNet NetOps provides assured network and information system availability, information protection, and information delivery across strategic, operational, and tactical boundaries.

- Network and information system availability. Provide visibility and control over the system and network resources. Effectively managing resources includes anticipating and mitigating problems. Proactive NetOps ensure uninterrupted availability and protection of the system and network resources. This includes providing for degradation, self-healing, diversity, and elimination of critical failure points.
- Information protection. Provide protection for the information passing over networks from the time it is stored and catalogued until distribution to the users, operators, and decisionmakers.
- Information delivery. Provide information to users, operators, and decisionmakers in a timely manner. NetOps personnel continuously monitor the networks to ensure the transfer of information is within the correct response time, and that throughput, availability, and performance meet the user's needs.

3-40. Figure 3-3 on page 3-10 establishes a common understanding of the relationships between NetOps activities and their individual and combined effects. The center of the figure illustrates LandWarNet NetOps tasks, their relationships with one another, their integration with the corresponding Department of

Defense information network operations tasks, and the desired effects once transformed into an integrated NetOps capability. The arrow in the figure illustrates how LandWarNet NetOps enables fusion across the DODIN, and enables knowledge managers to get the right information to the right user at the right time with the right protection.

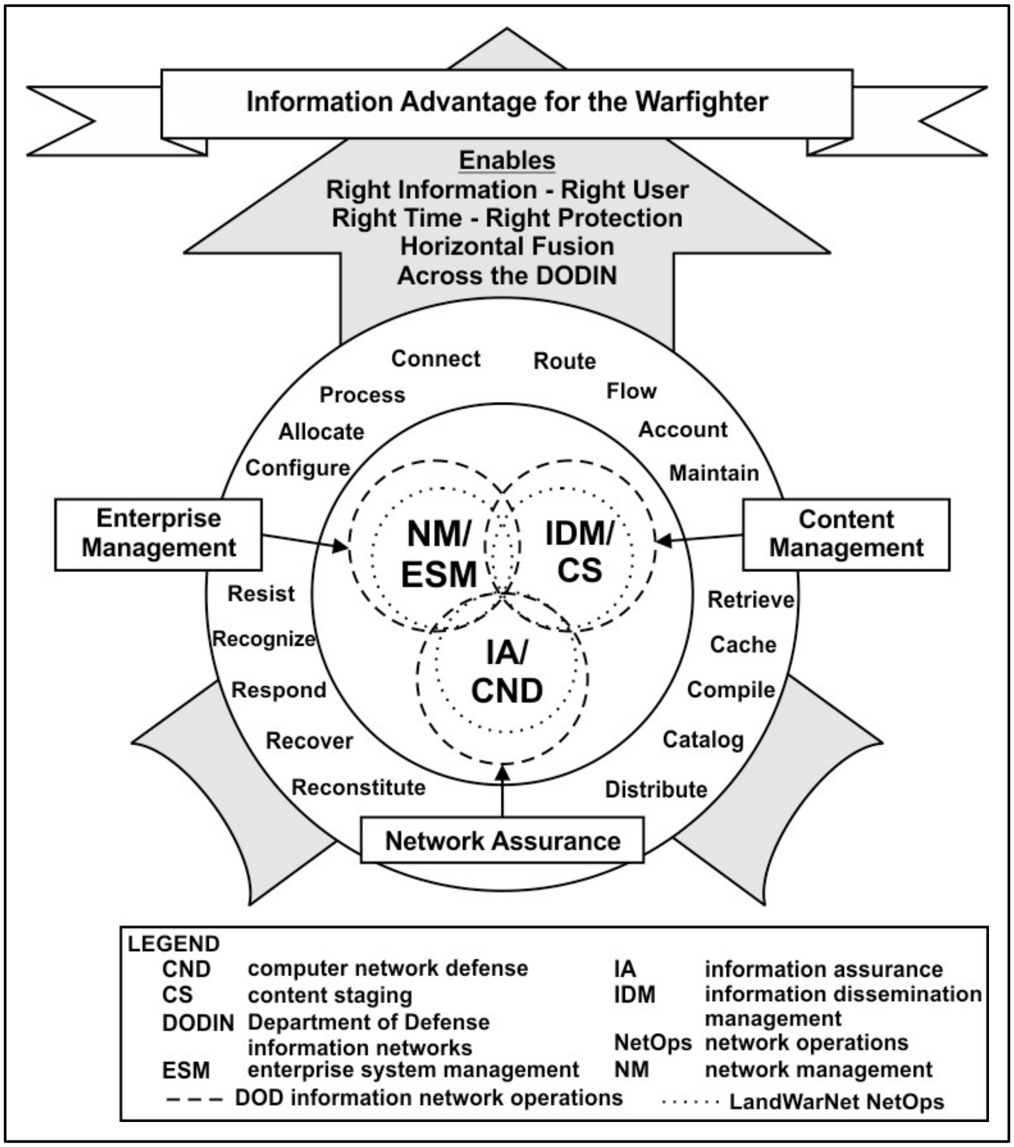

Information Advantage for the Warfighter
Enables
Right Information - Right User
Right Time - Right Protection
Horizontal Fusion
Across the DODIN
Connect
Route
Process
Flow
Allocate
Account
Configure
Maintain
Enterprise Management
Content Management
NM/ ESM
IDM/ CS
IA/ CND
Resist
Retrieve
Recognize
Cache
Respond
Compile
Recover
Catalog
Reconstitute
Distribute
Network Assurance
LEGEND
CND computer network defense
CS content staging
DODIN Department of Defense information networks
ESM enterprise system management
IA information assurance
IDM information dissemination management
NetOps network operations
NM network management
– – – DOD information network operations
· · · · · · LandWarNet NetOps

Figure 3-3. NetOps components, effects, and objectives

3-41. LandWarNet NetOps is the integration of the individual capabilities associated with NM/ESM, IA/CND, and IDM/CS that provides commanders the ability to harness the power of the DODIN and bring this power to their area of operations in order to shape and influence operations.

SECTION IV – CYBER THREATS

3-42. Defending LandWarNet and protecting the information on LandWarNet from threats is a responsibility of the Signal Corps and essential to freedom of action within the cyberspace domain. According to the Interagency Working Group on Cyber Security and IA, a cyber threat is any circumstance or event with the potential to, intentionally or unintentionally, exploit one or more vulnerabilities in a system resulting in a loss of confidentiality, integrity, or availability. As defined here, cyber threats not only involve an action but also require actors (threat agents) to execute that action in order to exploit cyber weaknesses.

3-43. Enemies and adversaries include, but are not limited to, nation-states, terrorists, hackers, internal users, and organized crime. They use different methods to deny, degrade, destroy, exploit, alter or otherwise adversely affect the Army's use of cyberspace. Because LandWarNet consists of many different segments existing across traditional domains, with many different means of communicating and differing levels of interconnectivity and isolation, a wide continuum of capabilities are available to the enemy to conduct cyber attacks. These capabilities target any portion of LandWarNet, ranging from particular physical nodes and links to the actual data residing in those nodes and links.

3-44. The adversary or enemy may continuously attempt to gather intelligence within LandWarNet in order to execute effective offensive operations. Successful intelligence gathering requires access to friendly activities and networks. Computer network exploitation and electronic warfare support are two types of intelligence operations performed within cyberspace and the electromagnetic spectrum. Computer network exploitation reveals information resident on or in transit through a system. Adversarial intelligence operations can reveal vital information about Army cyberspace operations.

3-45. Methods adversaries and enemies use to deny friendly use of the cyberspace domain and the electromagnetic spectrum include computer network attack (digital attack against logical networks), electronic attack (jamming of the electromagnetic spectrum), physical attack against infrastructure and electronics, as well as exploitation activities against computer networks or the electromagnetic spectrum.

- Computer network attack is the employment of network-based capabilities to destroy, disrupt, or corrupt information resident in or transiting through networks. Computer network attacks are entirely dependent on access to the target network. This sometimes requires capabilities specifically designed for the purpose of providing or enabling that access.
- Electronic attack is the subdivision of electronic warfare actions to prevent or reduce the effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception. Electronic attack uses electromagnetic energy, directed energy, and anti-radiation weapons to attack personnel, facilities or equipment with the intent of degrading, neutralizing, or destroying the enemy's combat capability.
- Physical attack uses measures to physically destroy or otherwise adversely affect a target. Because networks in cyberspace can be isolated, the ability to attack a network node physically may still be required. Physical attack can create effects within and outside cyberspace to help control the domain. Regardless of the degree of isolation, the adversary or enemy may determine a direct physical attack is the best option depending on the situation, the desired effect, and availability and suitability of other capabilities or options.

3-46. In considering the threat, the following must be factored—

- Cyberspace provides an adversary a greater level of obscurity in which to create a false sense of trust.
- Interconnectivity exposes critical infrastructures to the risk of perpetual cyber attacks mounted in cyberspace by adversaries.
- Expect rises in attacks by adversaries and enemies as convergence of network and device technologies accelerates and systems increasingly connect to the Internet.
- Resources for potentially harmful attacks are readily available, relatively inexpensive, and provide the adversary the ability to circumvent the need to regroup, refit, and reconstitute.
- Adversaries are capable of launching harmful attacks on Army systems, networks, and information assets by commandeering the use of unsuspecting systems and integrating them into the overall cyber arsenal.
- Individuals and organizations worldwide can access systems and networks connected to the Internet across geographic and national boundaries.
- Sensitive information tends to be isolated from the unsecure network. However, the various gateways that exist to facilitate transfer of information from the outside into a closed network provide many attack vectors susceptible to exploitation.

This page intentionally left blank.

Appendix A
Visual Information

Global Force Management is the predictive, streamlined and integrated process to manage the allocation and appointment of deployed forces, including Combat Camera (COMCAM) personnel. Global Force Management enables the Secretary of Defense to make proactive, informed management decisions by evaluating risk to the services and allocating appropriate forces to known requirements.

PROCEDURES FOR REQUESTING VISUAL INFORMATION SUPPORT

A-1. Combatant Command planners develop requirements and submit them to Joint Chiefs of Staff through their J-1/J-3 by entering the requirement into the joint capabilities and requirements manager. All rotational and emergent COMCAM requirements for joint operations vetting transpires through the Global Force Management process to the service providers. Once the appropriate Service sources the requirement, the details (personnel and logistics) are loaded in the Joint Operation Planning and Execution System for assignment of unit line numbers.

A-2. COMCAM support may come from any Services' COMCAM unit or activity. COMCAM forces, until placed under the operational or tactical control of deployed forces, belong to their particular Service. Prior to sending a tasking message—

- Make verbal contact with the COMCAM unit to discuss the type of support and timeframe of the required support. Coordinate as soon as possible with the COMCAM unit to ensure they can meet your needs.
- The COMCAM unit determines feasibility to support the requirement. In the event that COMCAM cannot meet the requesting unit's requirements, COMCAM assists in finding other resources that can support the requirements.

Note. Verbal contact is not a commitment or an agreement to provide support.

A-3. The requesting unit submits an official tasking using the following message tasking format—

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//
9th SIG CMD/NETCOM FT HUACHUCA AZ//G3//
7th SIG CMD (THEATER) FT GORDON//NETC-SFC-OPY (G3)//
21st SIG CMD 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:

Procedures for Requesting Visual Information Products

A-4. Complete government requests on official letterhead signed by a branch or unit head and submit by fax, mail or E-mail to the Defense Imagery Management Operations Center.

A-5. The following information is required when requesting imagery—

- Subject and/or image ID number.
- Unit, location, event, operation name.
- Date or date range.
- Equipment or equipment type to be depicted (if any).
- What action you want to see.
- Media format, size, and quantity.
- Date needed.
- Your name, rank, and position title.
- Your telephone numbers (DSN and commercial).
- Complete official mailing address that includes a building/room number or suite.
- How media is used (briefing, training).
- For motion media requests, include the approximate total number of minutes needed for each subject.
- Defense Imagery Management Operations Center provides still imagery through the defense imagery web site via zip file of high-resolution photographs for download onto your computer. (Duplication from that point is at the requestor’s own expense.)
- Official government customers can also obtain copies of visual information products from the defense imagery website at http://www.defenseimagery.mil/index.html.

Appendix B

Communications Security Procedures

Secure communications require key, device and other COMSEC material management at the lowest echelon possible while maintaining the highest physical and information security level the equipment and material require. This appendix provides the procedures to execute a COMSEC Incident Report, COMSEC Effective Status Message, accountability, and destruction by operational elements and users at all echelons.

PROCEDURES FOR COMMUNICATIONS SECURITY INCIDENT REPORT

B-1. It is the policy of the U.S. Government to safeguard and control COMSEC materials in a manner to assure continued integrity, prevent access by unauthorized persons, and control the spread of COMSEC materials, techniques, and technology when not in the best interest of the U.S. and its allies. The ultimate responsibility of safeguarding COMSEC material rests with the individual in possession of the material. Within Army organizations, this responsibility rests with the commander.

B-2. The G-6/s-6 uses a warning order to initiate the signal planning process for COMSEC equipment and material. Employ new COMSEC material in accordance with information on the warning order. The list includes the type of COMSEC material required. The G-6/S-6 verifies COMSEC and coordinates signal support as required.

B-3. During unified land operations, the Service authority is the command headquarters G-2, or activity within each military Service, overseas COMSEC operations, policy, procedures, and training. The Headquarters, Department of the Army Deputy Chief of Staff, Intelligence (G-2) serves in this capacity. The Service authority oversees the COMSEC Incident Monitoring Activity or processes and has final adjudication authority in determining if reported COMSEC incidents have resulted and are then responsible to report them to the National Security Agency for final adjudication.

B-4. Attempts to minimize or conceal violations or compromises of COMSEC jeopardize the operational security of communication and information systems.

B-5. In order to conduct a proper evaluation of a COMSEC incident, it is vital that all immediately available and essential information be included in the initial report. Do not delay incident reports in order to obtain additional information.

> ***Note***. The Headquarters, Department of the Army DCS G-2 has delegated functional Service authority responsibilities to Communications Security Logistics Activity, which serves as the Army COMSEC material central office of record and the Communications Security Incident Monitoring Activity (CIMA).

B-6. Prepare and submit all COMSEC reports in accordance with AR 380-40 and TB 380-41. Submit incident reports via the web-based COMSEC Incident Management Monitoring System (combat conditions exempted). This is the only official means of submitting COMSEC incident reports for all Army organizations to the COMSEC Incident Monitoring Activity and other recipients designated by the user. COMSEC Incident Management Monitoring System prompts the user for the information required to complete a COMSEC incident report and has a help feature to assist users to navigate the application. Other than combat situation, submit all reports using the COMSEC Incident Management Monitoring System.

B-7. The following is the COMSEC Compromise reporting checklist—

- Unit.
- Date-time group (DTG) reported.

- DTG of compromise.
- Controlled Cryptographic item (CCI) compromised.
- COMSEC/net IDs compromised.
- Probability of zeroed/destroyed.
- Eyewitnesses.
- First line S-6 assessment.

B-8. There are four types of COMSEC incidents that must be reported—

- **Physical incidents** include the loss, theft, loss of control, improper preparation of, or lack of preparation of, destruction reports (including supporting documentation for destruction reports) for COMSEC material. The capture, recovery by salvage, tampering, or unauthorized viewing, access or photography of classified COMSEC material or unclassified key marked "CRYPTO" are also physical incidents requiring a report. CCI, keyed or unkeyed, are included and reported accordingly.
- **Personnel incidents**. Any attempted recruitment, known or suspected contact by a foreign intelligence entity, capture by the enemy, or unauthorized absence or defection of an individual having knowledge of and access to COMSEC information or material are considered personnel incidents. The unauthorized disclosure or suspected disclosure of COMSEC information by individuals, or attempts by unauthorized persons to affect such disclosure, also fall into this category.
- **Cryptographic incidents**. Any equipment or software malfunction, human error by an operator or COMSEC account manager that adversely affects the cryptographic security of a machine, auto-manual, or manual cryptosystem is a cryptographic incident. Unique incidents, which pertain to specific cryptosystems, are contained in technical manuals, operational security doctrine or in specific DA pamphlets.
- **COMSEC administrative discrepancy** is administrative and COMSEC sensitive in nature as both are insecure practices dangerous to security, jeopardizing the integrity of COMSEC material. Because of this danger, it is essential that commanders take positive action to prevent their recurrence. Report these incidents within the Army chain of command as directed by command authorities, to cryptographic key controlling authorities or command authorities, and to the Communications Security Logistics Activity via the COMSEC Incident Management Monitoring System.

Note. Refer to TB 380-41, *Procedures for Safeguarding, Accounting, and Supply Control of COMSEC Material*, for more information on types of incident reports.

B-9. COMSEC incident reports constitute official command correspondence and are submitted by, or for, the commander. Use direct channels to ensure receipt of the report within the required period. COMSEC incident reports contain all information required by TB 380–41. Reporting commanders are responsible for notifying their chain of command that a COMSEC incident has occurred. Classification of COMSEC incident reports are according to content. Mark unclassified reports "For Official Use Only (FOUO)" and exempted from automatic disclosure under the provisions of AR 25–55.

Report Precedence and Timeliness

B-10. The following paragraphs indicate the message precedence for addressees and report submission times. Reports not submitted within the prescribed periods will contain an explanation for the delay.

B-11. Submit the following initial reports to the CIMA within 24 hours of discovery of the incident; at immediate precedence for action addressees and routine precedence for information addressees—

- Currently effective key or key scheduled to become effective within 15 days.
- Possible defection, espionage, clandestine exploitation, tampering, sabotage, or unauthorized copying, reproduction, or photographing.
- Recently superseded key (within 30 days).

B-12. Submit initial reports to the CIMA within 48 hours of discovery of the incident and at priority precedence for the following—

- Future key scheduled to become effective in more than 15 days.
- Superseded (more than 30 days ago), reserve, or contingency key.

B-13. Report initial COMSEC incident not covered in previous paragraphs within 72 hours of discovery of the incident, normally at routine precedence. However, if the incident has significant potential impact, originators should assign higher precedence.

B-14. Assign routine precedence to amplifying and final reports. However, assign a higher precedence if they contain significant new information affecting the evaluation of the incident reports.

B-15. The following is an example and instructions to complete a CCI Incident Report message—

UNCLASSIFIED EXAMPLE TO REPORT CCI INCIDENT REPORT

CONFIDENTIAL

FM: (COMPLETE MESSAGE ADDRESS)

TO: DIRUSACSLA FT HUACHUCA AZ//SELCL-IN//

INFO: (SEE TABLE 7-1, TB 380-41)

DTG: 221800Z SEP 05

CONFIDENTIAL (CLASSIFICATION IS BASED ON CONTENT)

SUBJECT: INITIAL/FINAL COMSEC INCIDENT REPORT (U)

A. (U) AR 380-40, CHAPTER 7, DTD XXXX

B. (U) TB 380-41, PARAGRAPH 5.24 THROUGH 5.33, DTD XXXX

C. (U) DA PAM 25-380-2

D. (U) AR 710-2

1. (U) DODAAC OF THE UNIT INVOLVED.

2. (C) MATERIAL IDENTIFICATION. COMPLETE IDENTIFICATION OF THE MATERIAL INVOLVED IN THE INCIDENT, INCLUDING— NOMENCLATURE, SERIAL NUMBER, AND QUANTITY. INDICATE WHETHER EQUIPMENT WAS KEYED OR UNKEYED.

3. (C) INCIDENT DESCRIPTION. PROVIDE A DESCRIPTION OF THE INCIDENT, INCLUDING THE DATE AND TIME OF DISCOVERY, AND ANSWERS THE QUESTIONS WHO, WHAT, WHEN, WHERE, WHY.

4. (U) COMPROMISE. ESTIMATE THE PROBABILITY OF POSSIBLE COMPROMISE, I.E., COMPROMISED, COMPROMISE CANNOT BE RULED OUT, OR NO COMPROMISE.

5. (U) KEY. IF KEY IS INVOLVED, IDENTIFY THE (CONTROLLING AUTHORITY) CONAUTH(S).

6. (U) MISSING CCI. IF THE MATERIAL INVOLVED IS MISSING, ALSO INCLUDE THE FOLLOWING:

(THE LOSS OF CCI REQUIRES AN AR 15-6 INVESTIGATION IAW AR 735-5, PARAGRAPH 13-2A (6)).

A. DATE, LOCATION AND CIRCUMSTANCE. LIST THE DATE, LOCATION AND CIRCUMSTANCES OF THE LAST KNOWN SIGHTING.

B. CAUSE OF LOSS. LIST ALL AVAILABLE INFORMATION PERTAINING TO THE CAUSE OF THE LOSS.

C. ACTIONS TAKEN. LIST ALL ACTIONS BEING TAKEN TO LOCATE THE MATERIAL.

D. POSSIBLE TAMPERING. INDICATE THE POSSIBILITY OF ACCESS BY UNAUTHORIZED PERSONS.

7. (U) TEMPORARY LOSS. IF THE MATERIAL WAS TEMPORARILY LOST OR OTHERWISE OUT OF PROPER CHANNELS ALSO INCLUDE THE FOLLOWING: A. TIME AND CIRCUMSTANCES. INDICATE THE EXACT PERIOD OF TIME AND UNDER WHAT CIRCUMSTANCES THE MATERIAL WAS DISCOVERED TO BE OUT OF PROPER CHANNELS.

B. ACTION. INDICATE THE ACTION WHICH CAUSED THE MATERIAL TO BE RETURNED TO PROPER CHANNELS.

C. CLEARANCE STATUS. INDICATE THE CLEARANCE STATUS OF PERSONS HAVING UNAUTHORIZED ACCESS.
D. SURREPTITIOUS ACCESS. INDICATE THE POSSIBILITY OF SURREPTITIOUS ACCESS BY UNAUTHORIZED PERSONS.
8. (U) INCLUDE CORRECTIVE ACTIONS IMPLEMENTED TO PREVENT A RECURRENCE OF THIS INCIDENT.
9. (U) POC. GIVE NAME, DSN, COMPLETE COMMERCIAL TELEPHONE NUMBER, FAX NUMBER, AND EMAIL ADDRESS.

UNCLASSIFIED EXAMPLE TO REPORT A CCI INCIDENT REPORT

B-16. Investigations: Normally, informal inquiries about reportable COMSEC incidents uncover sufficient information to determine if a compromise occurred and to recommend measures for preventing recurrence. Formal investigations may be required to determine certain violations of law or regulations. Conduct such investigations as mandated by regulation per direction of a cognizant higher authority, or at the discretion of the commander. Conduct investigations according to AR 15-6. Ensure investigating personnel have the appropriate security clearance.

B-17. Evaluations: Base the evaluation on information contained in an incident report, taking into consideration the security characteristics of the cryptosystem. Evaluations of incident reports must determine possible impact of the incident on all affected elements. The evaluation consists of CIMA personnel contacting the involved parties to determine if there were extenuating factors that led to the compromise or loss of control of the material in question. Consider the following evaluation factors—

- As the principal activities responsible for evaluation of COMSEC incidents, NSA and the Army CIMA may direct further investigation or reporting in order to ensure a proper evaluation.
- When evaluation of the incident indicates that supersession of any material is necessary, the controlling authority must immediately notify all holders of that item.
- A cryptosystem declared compromised will not be used for further encryption unless it is operationally essential that encrypted messages are sent before the supersession date and an alternate system is not available. See also AR 380-40, paragraphs 6-12 and 6-13.

B-18. COMSEC incident evaluation is often a subjective process, even when all pertinent facts are known. The guidelines below provide consistency in allowing the CIMA to assess commonly encountered types of incidents.

- Evaluate the following incidents as “COMPROMISE” and forward to NSA—
  - Lost keying material – This includes keying material believed destroyed without documentation, and material temporarily out of control.
  - Material believed lost, but later recovered under circumstances when unsure of continuous secure handling or found in an unauthorized location.
  - Unauthorized access – Access exists when a person has the capability and opportunity to gain detailed knowledge of, or to alter information or material/equipment. A person does not have access if the individual is under escort or if physical controls prevent detailed knowledge or altering of information or material.
  - Reports indicating the theft or loss of keying material or the defection of personnel – Under such circumstances, the CIMA must consider the material compromised and direct the controlling authority to initiate emergency supersession at the earliest practical time.
- Evaluate the following incidents as “COMPROMISE CANNOT BE RULED OUT” and forward to NSA—
  - When information provided in the incident report indicates that COMSEC material was possibly available to an unauthorized person, but there is no clear proof that it was available.
  - Unauthorized absence of personnel who have access to keying material. Furthermore, when a person who had access to keying material is officially reported

absent without authorization, all material the individual could access must be inventoried and the results of the inventory included in the report.

- Evaluate incidents involving local communication security management software, hardware or systemic failure as follows—
  - If a current back-up tape is available for the restoration of electronic key and the key management database, the CIMA shall rule the incident as “NO COMPROMISE” and not forward the report to NSA. As such, the CIMA requires no further investigation and notifies the account and the COMSEC office of record of these findings.
  - If the system must be restored using a non-current back-up tape, the CIMA shall consider any loss of COMSEC material and accounting records as a physical COMSEC incident. The CIMA forwards the final report to NSA with an evaluation that “COMPROMISE CANNOT BE RULED OUT” and notifies the COMSEC office of record of their findings.

Note. Complete guidelines for evaluating incidents involving joint staff positive control material and devices are contained in joint guidance governing positive control of material and devices.

B-19. Each COMSEC account must maintain case files for reportable COMSEC incidents. As a minimum, every case file includes—

- The initial/final report(s) as well as any amplifying reports. The initial report, or an amplifying report, could serve as the final report.
- The CIMA case assignment message. If not received within 30 days, the COMSEC account manager must follow-up with the CIMA to ensure the incident report was received and to request the case status.
- The COMSEC incident evaluation issued by the appropriate agency.
- The case closure message issued by CIMA.
- Retain COMSEC incident reports on file by COMSEC accounts for two years after closure to facilitate review by command inspectors and auditors. The Army CIMA maintains incident report files in the Communications Security Logistics Activity records holding area for no longer than six years and then destroys the report.

Note. For more information on reporting procedures, see TB 380-41, *Security: Procedures for Safeguarding, Accounting and Supply Control of COMSEC Material*.

PROCEDURES FOR COMMUNICATIONS SECURITY EFFECTIVE STATUS MESSAGE

B-20. Procedures to produce a COMSEC Effective Status Message are in TB 380-40, Appendix D. Effective and supersession dates classification are CONFIDENTIAL at a minimum and the controlling authority or command authority may upgrade the classification level.

B-21. The following is an example of a COMSEC Effective Status message—

UNCLASSIFIED
(NOTE: CONFIDENTIAL WHEN FILLED IN)
FM: CONAUTH 123 AMS (6C1234) YOUR AB PI
TO: ALL AUTHORIZED USERS
DIR TIER1 FT HUACHUCA AZ//KMT//(CONAUTHs reports to Tier 1)
INFO: IMMEDIATE SUPERIOR IN COMMAND
DIRNSA FT GEORGE G MEADE MD //I5107//
NCMS WASHINGTON DC (Navy/USMC/USCG/MSC accounts)
CMIO NORFOLK VA (Navy/USMC/USCG/MSC accounts)
MAJOR COMMAND
OTHER CONAUTHS (AS REQUIRED)
CLASSIFICATION: (MINIMUM OF CONFIDENTIAL)

SUBJ/COMSEC EFFECTIVE STATUS MESSAGE (U)//
REF/A/DOC/CONAUTH GUIDANCE/KMSP/DATE//
REF/B/DOC/CNSSI 4006/DATE//
NARR/REF A IS XXXXXXX. REF B IS XXXXXX.//
POC/NAME/POSITION/PHONE NUMBER/EMAIL ADDRESS//
RMKS/1. (C/REL) THE FOLLOWING INFORMATION IS REQUIRED:
(A) PARAGRAPH MARKING/RELEASE CODES
(B) SHORT TITLE
(C) CLASSIFICATION OF KEYMAT
(D) ASSOCIATED EQUIPMENT
(E) ALGORITHMS
(F) EDITION
(G) KEY CHANGEOVER TIME
(H) RELEASE COUNTRIES
(I) CONAUTH POINT OF CONTACT INFORMATION
REQUIRED FIELDS:
2. (C/REL) (SHORT TITLE) / (CLASSIFICATION) / (ASSOCIATED EQUIP) / (EDITION) / (KEY CHANGEOVER TIME)
SEGMENT NUMBERS / (DAILY, WEEKLY, MONTHLY, ETC) /
SEGMENT 01 / (CRYPTOPERIOD) / (SUPERSESSION DATE) /
EXAMPLE:
1. (C/US ONLY) AKAT/USKAD-1234/SECRET/KY-57/AB/0001Z/
1-12 ACTIVE SEGMENTS, 13-16 SPARES/WEEKLY/
SEGMENT 01/01-07 NOV 07/08 NOV 07/
SEGMENT 02/08-14 NOV 07/15 NOV 07/
SEGMENT 03/15-21 NOV 07/22 NOV 07/
2. (C/REL) ASAT-1234/SECRET/KY-57/AB/0001Z/
1-12 ACTIVE SEGMENTS, 13-16 SPARES/WEEKLY/ REL TO:
SEGMENT 01/01-07 NOV 07/08 NOV 07/
SEGMENT 02/08-14 NOV 07/15 NOV 07/
SEGMENT 03/15-21 NOV 07/22 NOV 07/
3. (U) CONAUTH GENERAL REMARKS CONCERNING EMERGENCY POCS, ETC.//
DECL/X1//
BT

COMSEC Accountability and Destruction

Accountability

B-22. All keying material is under accounting controls throughout its life cycle, from the moment generated, and upon receipt until final disposition through issue, transfer, or destruction. Accounting procedures are contained in TB 380–41. The Tier 1 COMSEC Army central office of record maintains a record of all accountable COMSEC material issued to COMSEC accounts. Continuously control centrally accountable key from time of receipt or generation through final disposition. A physical inventory of this key must be reconciled with the Army central office of record every six months.

Destruction of Communications Security Material

B-23. The destruction official and the witness must have a clearance equal to the highest classification of material for destruction. Both individuals must be physically present to view the actual destruction. Both are responsible for a properly prepared destruction report that lists all material destroyed and for ensuring that all destruction meets the appropriate standards in TB 380–41. Intentional falsification of COMSEC material destruction reports is subject to administrative and civil sanction, including adverse personnel actions, or criminal sanctions under the Uniform Code of Military Justice or Federal law, as appropriate.

B-24. Destroy superseded key material within 12 hours of supersession. Do not destroy defective or faulty key and immediately report it to the NSA IA Director and hold for disposition instructions.

B-25. The COMSEC account manager and alternate COMSEC account manager perform monthly or routine destruction of superseded editions of key. However, this routine scheduled destruction is not to be used as the basis for delaying immediate destruction of key no longer needed. Granting the authority to destroy superseded material to additional appropriately cleared people, who then certify this destruction to the COMSEC account manager, is preferable to delaying destruction even for a short period.

Destruction Schedule and Methods

B-26. Destroy issued keying material designated cryptographic material following expiration of the crypto period, or in accordance with the equipment operating instruction. Generally, key material may not be held longer than 12 hours following expiration of the crypto period. However, where special circumstances prevent compliance with the 12–hour standard, local commanders or responsible officials may grant an extension in writing up to 72 hours. In the case of an extended holiday period (more than 72 hours) or when special circumstances prevent compliance with the 12–hour standard (for example, destruction facility or operational space not occupied) destruction may be extended until the next duty day. In such cases, destroy the material as soon as possible after reporting for duty. Used or superseded keying material or extracts carried aboard special purpose aircraft may be retained in secure storage until secure destruction facilities are available, but must be destroyed as soon as possible thereafter.

B-27. Burning, disintegrating, crosscut shredding, or pulping are the approved methods for the routine destruction of paper COMSEC and classified material. Burning, disintegrating, and chemical alteration are the approved methods for the routine destruction of non-paper and classified material. COMSEC key tape is composed of paper-mylar-paper. Destroy COMSEC key tapes by burning, disintegrating, and chemical alteration.

COMSEC Assistance to Foreign Governments

B-28. COMSEC keying materials, documents, and hardware cannot be released to foreign governments without approval of the Chairman Joint Chiefs of Staff, and of the Director, National Security Agency/Chief, Central Security Service. The approval process for the release of COMSEC materials, documentation, and hardware requires strict adherence to approval authority guidance. However, use of communication liaison teams attached to foreign military forces can alleviate the need to release COMSEC materials to foreign military forces.

This page intentionally left blank.

Glossary (Chapter Title)

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 publication are marked with an asterisk (*). The proponent publication for other terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

ASCC	Army Service component command
BCT	brigade combat team
BLOS	beyond line of sight
CCI	controlled cryptographic item
CIMA	Communications Security Incident Monitoring Activity
CIO	chief information officer
CND	computer network defense
COMCAM	combat camera
COMSEC	communications security
CONAUTH	controlling authority
CP	command post
CS	content staging
DISA	Defense Information Systems Agency
DISN	defense information systems network
DOD	Department of Defense
DOTMLPF	Doctrine, Organizations, Training, Material, Leadership, Personnel, Facilities
DRSN	Defense Red Switched Network
DSN	Defense Switched Network
ESB	expeditionary signal battalion
ESC	expeditionary signal company
G-2	(Army) Deputy Chief of Staff for Intelligence; (joint) Army or Marine Corps component intelligence staff officer (Army division or higher staff, Marine Corps brigade or higher staff)
G-3	(Army) assistant chief of staff, operations; (joint) Army or Marine Corps component operations staff officer (Army division or higher staff, Marine Corps brigade or higher staff)
G-6	(Army) assistant chief of staff for communications; (joint) Army or Marine Corps component command, control, communications, and computer systems staff officer.
GCC	geographic combatant commanders
IA	information assurance
IDM	information dissemination management
IDM/CS	information dissemination management/content staging
IT	information technology
J-6	communications system directorate of a joint staff; command, control, communications, and computer systems staff section

JASC	joint/area signal company
JIE	Joint Information Environment
JTF	joint task force
KM	knowledge management
LOS	line of sight
NEC	network enterprise center
NETCOM	Network Enterprise Technology Command
NetOps	network operations
NIPRNET	Nonsecure Internet Protocol Router Network
NM	network management
NOSC	network operations and security center
NSA	National Security Agency
OPCON	operation control
RNOSC	Regional Network Operations and Security Center
S-2	(Army) battalion or brigade intelligence staff officer (USMC) battalion or regiment intelligence staff officer
S-3	(Army) battalion or brigade operations staff officer (USMC) battalion or regiment operations staff officer
S-6	(Army) battalion or brigade communications staff officer
SATCOM	satellite communications
SC(T)	signal command (theater)
SIGCoE	Signal Center of Excellence
SIPRNET	SECRET Internet Protocol Router Network
***SMO**	spectrum management operations
TIN-E	tactical installation and networking company-enhanced
TNOSC	Theater Network Operations and Security Center
TSSB	theater strategic signal brigade
VTC	video teleconference

SECTION II – TERMS

communications security

(Joint) A component of information assurance that deals with measures and controls taken to deny unauthorized persons information derived from telecomunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material. (CNSSI No. 4009)

computer network defense

(Joint) Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks. (JP 6-0)

cyberspace

(Joint) A global domain consisting of the interdependent network of information technology infrastructure and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 1-02).

Defensive Cyberspace Operations

(DOD) Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. (JP 1-02)

Department of Defense information networks

(Joint) The globally interconnected, end-to-end set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. (JP 1-02)

Department of Defense information network operations

(Joint) Operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information networks. (JP 1-02)

information management

(Army) The science of using procedures and information systems to collect, process, store, display, disseminate, and protect data, information, and knowledge products. (ADRP 6-0)

knowledge management

(Army) The process of enabling knowledge flow to enhance shared understanding, learning, and decisionmaking. (ADRP 6-0)

***LandWarNet**

The Army's portion of the Department of Defense information networks. A technical network that encompasses all Army information management systems and information systems that collect, process, store, display, disseminate, and protect information worldwide.

network operations

(Joint) Activities conducted to operate and defend the Department of Defense information networks. (JP 6-0)

***network transport**

A system of systems including the people, equipment, and facilities that provide end-to-end communications connectivity for network components.

Offensive Cyberspace Operations

(Joint) Offensive cyberspace operations intended to project power by the application of force in or through cyberspace. (JP 1-02)

***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.

visual information

(Joint)The use of one or more of the various visual media with or without sound. (CJCSI 3205.01C)

This page intentionally left blank.

References

REQUIRED PUBLICATIONS

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

ADRP 1-02. *Terms and Military Symbols*. 24 September 2013.

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms*. 8 November 2010.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT PUBLICATIONS

Most joint publications are available online: http://www.dtic.mil/doctrine/new_pubs/jointpub.htm

CJCSI 3205.01C. *Joint Combat Camera (COMCAM).* 27 January 2010.

CJCSM 6231.01D. *Manual for Employing Joint Tactical Communications.* 15 January 2010.

CJCSM 6510.01B. *Cyber Incident Handling Program.* 10 July 2012.

CNSSI No. 4009. *National Information Assurance (IA) Glossary.* 26 April 2010.

DODI 8500.2. *Information Assurance Implementation.* 6 February 2003.

DOD O-8530.1-M. *Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Process.* 17 December 2003.

JP 3-27. *Homeland Defense*. 12 July 2007.

JP 6-0. *Joint Communications System*. 10 June 2010.

JP 6-01. *Joint Electromagnetic Spectrum Management Operations.* 20 March 2012.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: http://www.apd.army.mil

ADP 3-28. *Defense Support of Civil Authorities*. 26 July 2012.

ADRP 3-0. *Unified Land Operations*. 16 May 2012.

ADRP 6-0. *Mission Command*, Chg 1. 10 September 2012.

AR 5-22. *The Army Force Modernization Proponent System.* 6 February 2009. (RAR 25 March 2011)

AR 25-1. *Army Knowledge Management and Information Technology*. 25 June 2013.

AR 25-2. *Information Assurance*. 24 October 2007. (RAR 001 23 March 2009)

AR 25-6. *Military Affiliate Radio System (MARS) and Amateur Radio Program.* 01 May 2007.

AR 25-55, *The Department of the Army Freedom of Information Act Program*, 01 November 1997

AR 380-5. *Department of the Army Information Security Program.* 29 September 2000.

AR 380-40. *Safeguarding and Controlling Communications Security Material.* 9 July 2012 (RAR 24 April 2013)

AR 381-11. *Intelligence Support to Capability Development*. 26 January 2007.

AR 600-82. *The U.S. Army Regimental System*. 5 June 1990.

AR 700-131. *Loan, Lease, and Donation of Army Material*. 23 August 2004.

AR 735-5. *Policies and Procedures for Property Accountability*. 10 May 2013.

ATP 3-37.10. *Base Camps.* 26 April 2013.

ATTP 4-15. *Water Transportation Operation.* 11 February 2011.

FM 3-05.160. *Army Special Operations Forces Communications System*. 15 October 2009.

FM 3-14. *Space in Support of Army Operations.* Chg 1, 6 January 2010.

FM 6-01.1. *Knowledge Management Operations*. 16 July 2012.

FM 6-02.40. *Visual Information Operations*. 10 March 2009.

FM 27-10. *The Law of Land Warfare*. 18 July 1956.

TB 380-40. *Security: Army Controlling Authority and Command Authority Procedures.* 10 September 2012.

TB 380-41. *Security: Procedures for Safeguarding Accounting and Supply Control of COMSEC Material*. 16 November 2012.

PRESCRIBED FORMS

None

REFERENCED FORMS

Forms are available online: http://www.apd.army.mil

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

WEB SITES

Joint Capability Areas Web site http://www.dtic.mil/futurejointwarfare/jca.htm
Defense Imagery Web site https://www.defenseimagery.mil/index.html
C4IM Services List Web site https://www.itmetrics.hua.army.mil

Index

This index references the terms location by page number.

FM 6-02
22 JANUARY 2014

By order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

GERALD B. O'KEEFE
Administrative Assistant to the
Secretary of the Army
1401001

DISTRIBUTION:

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

PIN: 103938-000