ATP 6-02.71

TECHNIQUES FOR DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS

APRIL 2019

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

*This publication supersedes FM 6-02.71, dated 14 July 2009.

Headquarters, Department of the Army

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

Army Techniques Publication
No. 6-02.71

Headquarters
Department of the Army
Washington, DC, 30 April 2019

Techniques for Department of Defense Information Network Operations

Contents

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

*This publication supersedes FM 6-02.71, dated 14 July 2009.

Figures

Tables

This page intentionally left blank.

Preface

ATP 6-02.71, *Techniques for Department of Defense Information Network Operations*, describes the Army network and discusses the capabilities it extends to Army forces. It also discusses how the network enables command and control in Army operations.

The principal audience for ATP 6-02.71 is Army professionals and contractors whose duties involve installing, operating, maintaining, and securing the enterprise network. To apply this doctrine correctly, readers should be familiar with capstone Army doctrine (ADP 1 and ADP 3-0), FM 3-0, and FM 6-02.

Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable U.S., international, and, in some cases, host-nation laws and regulations. Commanders at all levels ensure that their Soldiers operate in accordance with the law of war and the rules of engagement. (See FM 27-10.) They also adhere to the Army Ethic as described in ADRP 1.

ATP 6-02.71 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. Terms for which ATP 6-02.71 is the proponent publication (the authority) are italicized in the text and are marked with an asterisk (*) in the glossary. Terms and definitions for which ATP 6-02.71 is the proponent publication are boldfaced in the text. For other definitions in the text, the term is italicized, and the number of the proponent publication follows the definition.

ATP 6-02.71 applies to the Active Army, Army National Guard/Army National Guard of the United States, and United States Army Reserve unless otherwise stated.

The proponent for this publication is the United States Army Cyber Center of Excellence. The preparing agency is the Doctrine Division, United States Army Cyber Center of Excellence. Send comments and recommendations on a DA Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Commander, United States Army Cyber Center of Excellence and Fort Gordon, ATTN: ATZH-ID (ATP 6-02.71), 506 Chamberlain Avenue, Fort Gordon, GA 30905-5735; by e-mail to usarmy.gordon.cyber-coe.mbx.gord-fg-doctrine@mail.mil.

This page intentionally left blank.

Introduction

ATP 6-02.71 is the primary doctrine publication for Department of Defense information network operations to support the Army's mission. ATP 6-02.71 augments the Department of Defense information network information provided in FM 6-02. This publication establishes non-prescriptive ways to perform missions, functions, and tasks associated with Department of Defense information network operations in Army networks to enable and support the Army's mission at all echelons. This publication nests with the doctrinal principles in FM 3-12, FM 6-02, JP 3-12, JP 6-0, and complements the tactical Department of Defense information network operations doctrine in ATP 6-02.53 and ATP 6-02.60.

The Signal Corps provides each geographic combatant commander the personnel and tools to collect, transport, process, protect, and disseminate information within their respective theater. This facilitates information advantage by enabling delivery of, and access to, the right information, at the right time, and in the right format. This manual provides a general understanding of Department of Defense and Army networks. Network operations and protection capabilities are critical to enable combat success and prevail in the information environment.

The vision for the Department of Defense information network-Army is the employment of an end-to-end network that provides assured global command and control and enables the Army's readiness and ability to fight and win in a contested and congested operating environment. This network seamlessly integrates services and capabilities from strategic to tactical echelons and enables all warfighting functions. The network is a warfighting platform that enables commanders to integrate joint combined arms and all elements of combat power. It supports leaders' ability to understand, visualize, and describe the operational environment, problems, and approaches to solving them. It also supports commanders' ability to make decisions and direct action toward a desired end state, and assess understanding of the problem, adequacy of the operational approach, and subsequent plans and level of progress.

The network is tailorable and will adapt, based on phases of an operation, to provide assured command and control at home station, while en route, and in deployed environments. Deployed environments include training, exercises, theater security cooperation, initial entry, and maneuver. Deployed environments may employ minimal to robust force packages, requiring the network to adjust to provide the right services at the point of need, under all conditions.

Signal formations will seek to deliver services at point of need and reduce the deployed footprint and operational risk through home station mission command. The ability to predict the actions of enemies and adversaries enables proactive defense and assures access to critical data and the security of Army networks and systems. This is essential to mission success.

The network must embrace common standards from a joint and multinational perspective that allow the addition of capabilities and systems while reducing, not increasing complexity of the network. The network must provide an advantage and not a burden while providing enhanced speed and agility to our warfighting formations. As capabilities evolve to make Army networks less complex and more defensible, the Cyber Center of Excellence will evolve doctrine to describe the current and effective employment of networks and systems in congested and contested operating environments. The Cyber Center of Excellence will update this publication as improvements and changes in capabilities occur, or when there are changes in the expected operating environment.

ATP 6-02.71 supersedes FM 6-02.71, *Network Operations*. ATP 6-02.71 is generally consistent with FM 6-02.71 on key topics and adopts updated terminology and techniques. As in FM 6-02.71, network operations (now referred to as Department of Defense information network operations) remains a core competency of the Signal Corps. This update includes the Department of Defense information network and Department of Defense information network-Army, the principles and components of Department of Defense information network operations, and the roles and responsibilities of various individuals, organizations, and elements. It also discusses the tiers and functions of Department of Defense information network operations control centers and the concepts and activities associated with Department of Defense information network operations.

ATP 6-02.71 has three chapters and one appendix.

Chapter 1 section I introduces the information environment and the challenges presented by operations in a contested and congested environment. Section II provides a brief overview of the network. It defines and discusses the global network, joint theater networks, and the Army network (strategic and tactical). Section III introduces Department of Defense information network operations, their critical tasks, and operation of Army networks. The section concludes with the transition of theater responsibilities through the joint operational phases.

Chapter 2 discusses Department of Defense information network operations roles and responsibilities from the national level to tactical echelons. Chapter 2 discusses those elements with global responsibilities, the elements and organizations that operate the theater network, and the corps and below units that provide and operate deployed networks.

Chapter 3 discusses Department of Defense information network operations activities. It elaborates on the tasks to install, operate, maintain, and secure Department of Defense networks. Chapter 3 also discusses network management and reporting requirements for shared network situational understanding.

Appendix A discusses the Department of Defense information network operations tasks of enterprise management, cybersecurity, and content management; their underlying principles and components; and shared network situational understanding. Appendix A discusses the components of Department of Defense information network operations and further defines each essential task.

Based on current doctrinal changes, certain terms for which ATP 6-02.71 is the proponent have been added, rescinded, or modified for purposes of this publication. The glossary contains acronyms and defined terms. See introductory table-1, introductory table-2, and introductory table-3 for specific term changes.

Introductory table-1. New Army terms

Term	*Remarks*
Department of Defense information network-Army (DODIN-A)	New term and definition (replaces LandWarNet)
network enterprise center	New term and definition

Introductory table-2. Rescinded Army terms

Term	*Remarks*
Army Communications Systems Operations	Rescinded
LandWarNet	Rescinded

Introductory table-3. Modified Army terms

Term	*Remarks*
technical channels	Modified definition

Chapter 1

Department of Defense Information Network-Army

This chapter introduces the Army's enterprise network. It discusses the fixed infrastructure strategic network that provides the network and transport backbone and introduces the tactical portion of the network. This chapter concludes by introducing Department of Defense information network operations, Department of Defense information network operations in the Army network, and the transfer of Department of Defense information network operations responsibilities through the joint operational phases.

SECTION I – THE INFORMATION ENVIRONMENT

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

CONGESTED ENVIRONMENT

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

CONTESTED ENVIRONMENT

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

1-4. U.S. forces dominated cyberspace and the electromagnetic spectrum in Afghanistan and Iraq against adversaries who lacked the technical capabilities to compel the coalition to contend with a contested environment. More recently, regional peers have demonstrated impressive capabilities in a hybrid operational environment. These adversary capabilities threaten U.S. freedom of action in cyberspace and the electromagnetic spectrum. Because communications are a key command and control enabler, U.S. military communications and information networks present high value targets for enemies and adversaries. Technologically sophisticated adversaries understand the extent of U.S. forces' reliance on communications and automated information systems. In future conflicts, we should expect our enemies and adversaries will contest the information environment to deny operational access and diminish the effectiveness of U.S. and allied forces.

1-5. Degraded capabilities may result from hostile threat actions, but may also occur due to insufficient resources for all forces in the operational area. They may also result from a lack of coverage—such as inadequate communications satellite capacity—in the operational area, or from electromagnetic interference, whether intentional (jamming) or unintentional.

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

1-7. U.S. military networks face continuous cyberspace risk from a variety of threat sources. Every day DOD networks come under attack by threat agents, including—

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

1-8. The persistent nature of the cyberspace risk causes U.S. forces to expend a great deal of resources and effort securing and defending DOD networks. Network-enabled operations are a force multiplier and a traditional strength of U.S. forces. But network-enabled operations also create significant vulnerabilities. The extent to which U.S. forces rely on networks and networked capabilities presents broad cyberspace and electronic warfare attack surfaces. Each network device and capability becomes a potential attack vector an adversary may seek to exploit. Failing to protect even one system can give an adversary a foothold into the Department of Defense information network (DODIN) and place sensitive data, U.S. operations, and lives at risk. Even when cyberspace defenders discover and stop an attack, it is not always possible to attribute the attack to a particular source. Following cybersecurity best practices, maintaining active cyberspace defense, and adhering to operations security guidelines help protect DOD networks and data.

SECTION II – NETWORK OVERVIEW

1-9. The DODIN follows global technical direction for operation and defense. DODIN operations functions take place at the global, theater, and installation (local) levels.

GLOBAL NETWORK

1-10. The *Department of Defense information network* is the set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems (JP 6-0). As the DOD portion of cyberspace, the DODIN interacts with and provides connections to national and global cyberspace. The DODIN encompasses the Service-specific enclaves of the Army, Navy, Air Force, and Marine Corps combined with joint capabilities provided by the Defense Information Systems Agency. An *enclave* is a set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter (CNSSI 4009). The DODIN provides Defense Information Systems Network (DISN) services, including SECRET Internet Protocol Router Network (SIPRNET), Non-classified Internet Protocol Router Network (NIPRNET), and video teleconferencing.

JOINT INFORMATION ENVIRONMENT

1-11. The joint information environment is a secure environment to share information technology (IT) infrastructure, enterprise services and a single security architecture within the DODIN. The joint information environment enables information advantage while improving mission effectiveness, increasing security, and producing IT efficiencies. *Information advantage* is the superior position or condition derived from the ability to securely access, share, and collaborate via trusted information while exploiting or denying an adversary's ability to do the same (DODD 8000.01). The joint information environment aligns theater DODIN operations with combatant command authorities. It uses enforceable standards and specifications, and common tactics, techniques, and procedures. The joint information environment improves operational effectiveness by standardizing training and technical requirements across combatant commands and geographic regions. This standardization enhances security and allows Services and DOD agencies to effectively allocate and align their IT resources.

Cloud Computing

1-12. 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. DOD components acquire cloud services through the Defense Information Systems Agency, or obtain a waiver from the DOD chief information officer designated review authority (FM 6-02).

THEATER NETWORK

1-13. A geographic combatant command operates in a clearly delineated area of responsibility (AOR) with a distinctive regional military focus. Signal planners plan communications and network capabilities to support all anticipated requirements in the operational area. However, in a degraded or denied environment, there may not be adequate communications capacity to support all missions. Changes in the operational or mission variables may change requirements beyond the ability of assigned and attached signal element capabilities. Theater DODIN operations responsibilities align to the operational chain of command for unity of command and unity of effort. This alignment allows commanders to allocate available communications and network support to their highest mission priorities until additional capabilities are available. The AOR's supporting Army Service component command (the theater army) provides the Army portion of the geographic combatant commander (GCC) operational force requirements.

1-14. The theater network consists of the systems and devices controlled by the combatant command and its Service components. The theater network provides in-theater access to DISN and theater-specific information services. The GCCs direct DODIN operations within their respective AORs.

ARMY NETWORKS

1-15. Military Departments and Services provide an interoperable and compatible communications system for the effective conduct of military operations and plan for the expansion of the DODIN to meet the requirements of DOD (JP 6-0). The ***Department of Defense information network-Army*** **is an Army-operated enclave of the Department of Defense information network that encompasses all Army information capabilities that collect, process, store, display, disseminate, and protect information worldwide**. The Department of Defense information network-Army (DODIN-A) includes all Army automated information systems and networks, including stand-alone networks supporting intelligence, sustainment, medical, Army National Guard, and United States Army Reserve.

1-16. The DODIN-A provides commanders the ability to conduct authorized cyberspace operations while continuing to enable command and control and support the other warfighting and business functions. It provides the means for the Army to collaborate internally and externally; move and manage information; send and receive orders; and maintain situational understanding across the formation of posts, camps, and stations into austere environments in joint AORs worldwide.

> ***Note.*** Department of Defense information network-Army (DODIN-A) replaces the term LandWarNet, which remains in some legacy Army policy and doctrinal publications.

FIXED INFRASTRUCTURE STRATEGIC NETWORK

1-17. Army personnel, strategic signal units, and facilities contribute to a centralized, secure, operational, and sustainable joint backbone network controlled by the Defense Information Systems Agency through the Joint Force Headquarters-DODIN (see paragraph 2-5). This strategic network provides dedicated voice, video, and data services to train and accomplish the Army's mission as a continental United States-based expeditionary force. The goal is for each unit to have the same services and mission command enabling applications while operationally deployed that they use in the garrison and training environments. Every Soldier, regardless of geographic location or deployment status, has a universal e-mail address, a single file storage medium, and standard collaboration tools. Units can deploy with their home station directory numbers.

1-18. The strategic network provides fixed infrastructure that not only supports operations in garrison but also provides access points to connect deployed tactical forces to the DODIN. The strategic network provides expeditionary forces reachback and access to DISN services, regardless of where their mission takes them. *Reachback* is the process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed (JP 3-30). Because the architecture and cybersecurity configurations are standardized across theaters, expeditionary units can enter a theater with their automated information systems preconfigured, ready to join the theater infrastructure and quickly establish communications and DISN services.

1-19. Figure 1-1 on page 1-5 shows the logical distribution of the fixed infrastructure strategic network. It does not illustrate the command and control relationships and technical channels. These elements form and govern the communications backbone that provides worldwide reach. The Army Cyber Operations and Integration Center (ACOIC) provides overall network oversight for the Army through United States Army Network Enterprise Technology Command (NETCOM) and the regional cyber center (RCC), and defensive cyberspace operations through the cyber protection brigade and the RCCs. The RCCs provide theater-level oversight for DODIN operations and cyberspace defense, and may or may not be colocated with the other elements of the network service center. The network service center provides services across a theater and serves as the access point to extend enterprise services to deployed users through the regional hub node. A functional network operations and security center (NOSC) (see paragraph 2-18) provides similar capabilities to an RCC, but aligns with a function, such as Army National Guard or special operations, rather than a geographic location. The joint regional security stack provides perimeter protection and connects installation campus area networks to the DODIN. The network enterprise center (NEC) provides DISN services on an installation. See chapter 2 for detailed information about the global, theater-focused, and installation-level DODIN operations organizations.

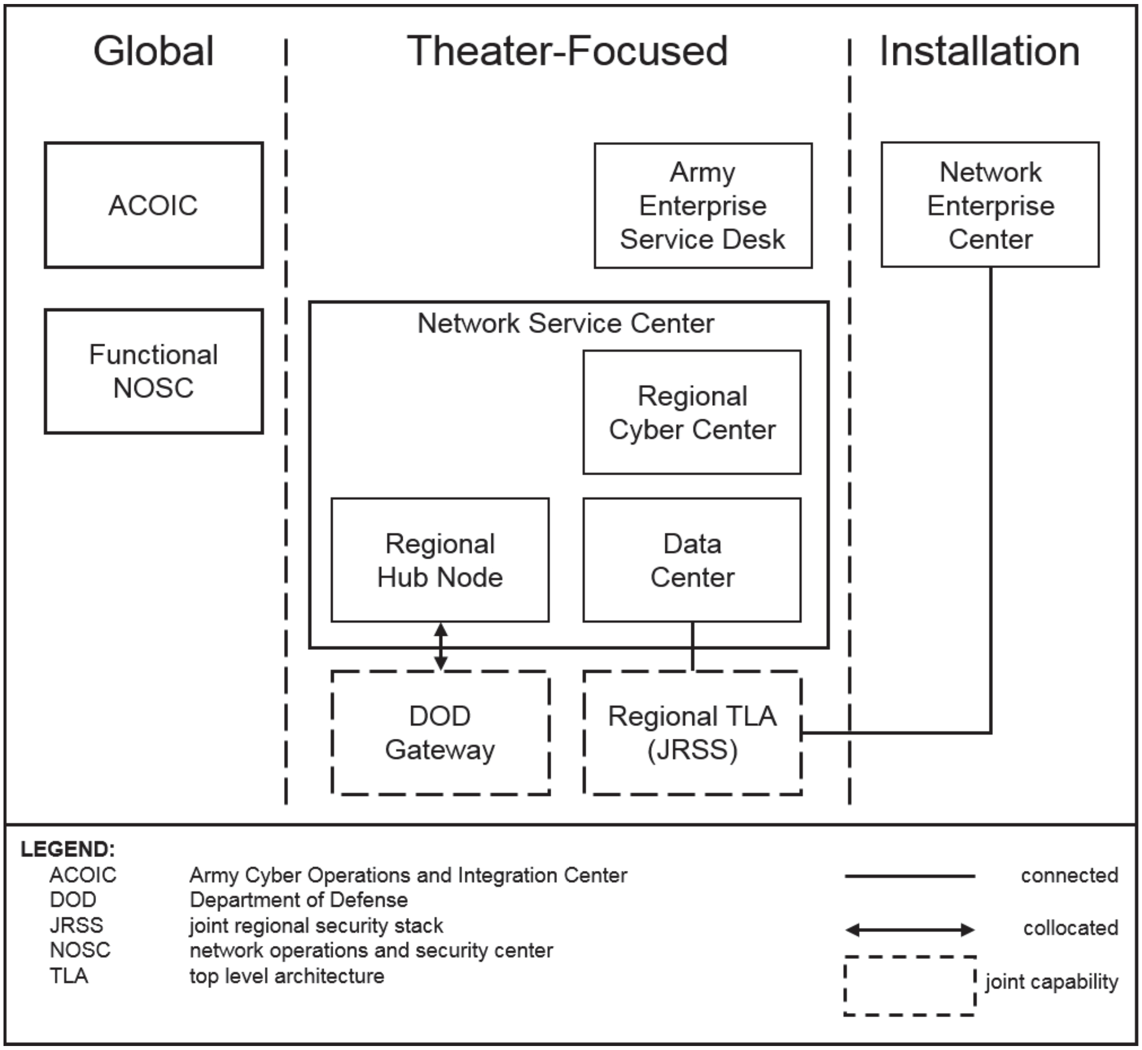

Global
Theater-Focused
Installation
ACOIC
Functional NOSC
Army Enterprise Service Desk
Network Enterprise Center
Network Service Center
Regional Cyber Center
Regional Hub Node
Data Center
DOD Gateway
Regional TLA (JRSS)
LEGEND:
ACOIC Army Cyber Operations and Integration Center
DOD Department of Defense
JRSS joint regional security stack
NOSC network operations and security center
TLA top level architecture
connected
collocated
joint capability

Figure 1-1. Fixed infrastructure strategic network

TACTICAL INTERNET

1-20. The tactical internet is the deployed portion of the DODIN-A. The deployed portion of the network is functionally similar to the commercial internet because the communications infrastructure uses many of the same technologies. The tactical internet extends the same classified and unclassified DISN services and mission command applications to deployed units that they use at their home station. From a management standpoint, the tactical internet divides into the upper and lower tiers.

1-21. DODIN operations responsibilities vary with the tiers. This publication focuses primarily on DODIN operations in the strategic network and upper tier tactical internet. See ATP 6-02.53 for further information on DODIN operations in the lower tier tactical internet.

Upper Tier

1-22. Warfighter Information Network-Tactical (WIN-T) (see paragraph 1-27) provides the upper tier tactical internet and connects the lower tier to the DODIN. At the corps and below, the upper tier tactical internet consists of WIN-T resources that provide high-throughput networking at-the-halt to corps command posts, and at-the-halt or on-the-move at the division, and brigade. The network transport capabilities for the upper tier are frequency division multiple access and time division multiple access satellite and line of sight terrestrial network transport.

1-23. The theater-pooled WIN-T resources of the expeditionary signal battalion (ESB) extend network services at-the-halt for those units not equipped with WIN-T.

1-24. The upper tier provides the gateway capability between the upper and lower tiers. It is an interoperability point for higher echelons, aviation integration, and interoperability with joint, inter-organizational, and multinational elements.

Lower Tier

1-25. The lower tier supports tactical formations down to the team leader. It consists primarily of single-channel radio networks at platoons and companies. The primary lower tier waveforms are the Soldier radio waveform and the single-channel ground and airborne radio system (see ATP 6-02.53).

1-26. The lower tier tactical internet provides transport for operational information. Mobile applications enable visualization, operator interface with ancillary devices (such as Global Positioning System), targeting data, voice communications, and sensor capability. WIN-T's combat net radio gateway provides a bridge to connect combat net radio voice networks to the upper tier. Two-channel radios integrate Soldier radio waveform and single-channel ground and airborne radio system networks.

Warfighter Information Network-Tactical

1-27. WIN-T is the Army's integrated tactical communications networking system. It provides automated radio network planning and integrates DODIN operations tools into the network infrastructure. WIN-T implements the tactical portion of the DODIN-A by combining line of sight radios and satellite communications transport with the following network management techniques:

- Defense-in-depth to provide multi-layer cybersecurity protection, from the division or brigade NOSC to the individual network nodes.
- Distributed (decentralized) network node management.
- Communications-in-depth with automatic rerouting.
- Self-forming and self-healing network (increment 2).
- Over-the-network radio management.

1-28. The self-forming and self-healing network architecture of WIN-T helps mitigate adversary effects when operating in a contested environment. The communications-in-depth architecture includes redundant network transport capabilities to dynamically recover and reestablish network connectivity if either the line of sight or the satellite communications link is disrupted. Because WIN-T uses Internet protocol (IP) routing, removing one node—even a key node—from the network does not interfere with the rest of the network's ability to communicate. DODIN operations tools integrated into the system architecture improve the tactical network's cybersecurity posture and enable monitoring of traffic for reporting to higher-level DODIN operations facilities. See ATP 6-02.60 for more information about WIN-T's self-forming, self-healing network architecture.

1-29. WIN-T platforms use quality of service enabled devices for efficient use of network bandwidth. These devices prioritize data traffic based on type and importance and preempt lower priority traffic when required.

1-30. WIN-T also includes a combat net radio gateway connection at selected nodes for the lower tier tactical internet. For more information on WIN-T, see ATP 6-02.60. For more information on the lower tier tactical internet, see ATP 6-02.53.

SECTION III – INTRODUCTION TO DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS

DEFINITION

1-31. *Department of Defense information network operations* are operations to secure, configure, operate, extend, maintain, and sustain Department of Defense cyberspace to create and preserve the confidentiality, availability, and integrity of the Department of Defense information network (JP 3-12). DODIN operations are one of the three cyberspace missions. The other cyberspace missions are defensive cyberspace operations and offensive cyberspace operations.

1-32. In the past, the Army and DOD have treated network operations as a task performed to manage the network. DODIN operations are not an individual or crew task, but multifaceted military operations that take place at all echelons. DODIN operations are arguably the most important and most complex type of operation the Army performs on a daily basis. The network is the foundational capability for all other Army warfighting functions and capabilities, including mission command; intelligence, surveillance, and reconnaissance; precision fires; logistics; and telemedicine. Commanders and their staffs conduct DODIN operations to leverage the network as a warfighting platform.

1-33. Besides providing the network to support mission command and all other warfighting functions, DODIN operations support and enable defensive and offensive cyberspace operations. Successful cyberspace operations require integrating and synchronizing all three types of cyberspace missions. See JP 3-12 and FM 3-12 for more information on defensive and offensive cyberspace operations.

CRITICAL TASKS

1-34. DODIN operations enable staffs at each echelon to execute commanders' priorities throughout the enterprise. DODIN operations allow commanders to communicate and collaborate effectively, and to share, manage and disseminate information using automated information systems. DODIN operations consist of three critical tasks (for more detailed information on the critical DODIN operations tasks, refer to Appendix A)—

- **DODIN enterprise management** is the technology, processes, and policies necessary to execute the DODIN operations functions to install, operate, maintain, secure, and restore communications networks, information systems, and applications. Enterprise management merges baseline IT services with DODIN operations capabilities. For more information on baseline services, see FM 6-02. Within Army networks, enterprise management is composed of network management and enterprise systems management.
- ***Cybersecurity*** is prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation (DODI 8500.01). Cybersecurity satisfies the DODIN operations function of securing DOD networks. Through cybersecurity, DODIN operations providers protect, monitor, analyze, detect, respond to, and report unauthorized activity within DOD information systems and computer networks.
- **DODIN Content management** allows DODIN operations personnel to optimize the flow and location of information over the DODIN by positioning and repositioning data and services to optimum locations on the DODIN relative to information producers, information consumers, and mission requirements. Content management enables knowledge management. In Army networks, content management is information dissemination management and content staging. For detailed information on information dissemination management and content staging see appendix A.

1-35. Shared visibility of DODIN operations status across the DODIN is critical to situational understanding and decision making. Shared network situational understanding, along with coordination between stakeholders on potential events, helps commanders and non-IT staff understand the impact of DODIN operations on their operational mission. Comprehensive network situational awareness identifies policy violations and facilitates network troubleshooting and restoral. Anomalous network activity may give the first indication of a cyberspace attack.

DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS IN ARMY NETWORKS

1-36. The Army conducts distributed DODIN operations within the DODIN-A, from the global level to the tactical edge. DODIN operations personnel install, operate, maintain, and secure from post, camp, or station to deployed tactical networks. DODIN operations provide assured and timely network-enabled services to support DOD warfighting, intelligence, and business missions across strategic, operational, and tactical boundaries. DODIN operations enable system and network availability, information protection, and information delivery.

1-37. Army personnel implement enterprise DODIN operations through an established hierarchy. The DODIN-A enables access to the right information at the right place and time, so commanders, staffs, Soldiers, civilians, and joint, inter-organizational, and multinational mission partners can meet mission requirements. The DODIN-A segments are home or mobile; post, camp, or station; and deployed tactical network. These segments allow operating and generating forces to access centralized resources from any location during all operational phases. Network support is available at the home post, camp, or station and throughout the deployment cycle.

1-38. The network service center includes data centers, DOD gateway facilities, and regional hub nodes. The network service center is the DODIN-A interface that connects Army users with joint services and applications. The network service center includes both joint and Army-unique capabilities (see figure 1-1 on page 1-5). The DOD gateway and long-haul satellite transport are joint capabilities that provide backbone connectivity and connection to DISN services. The data center and regional hub node are Army capabilities. The regional hub node provides the connection between deployed Army enclaves and the DODIN. For more information about the regional hub node, see ATP 6-02.60. For more information on DOD gateway, see JP 6-0 and ATP 6-02.54.

1-39. The data center provides a data repository for content staging, continuity of operations, and redeployment support. It also provides access for those users who access the network from home or a temporary duty location.

1-40. The post, camp, and station segment is the primary network access point while in garrison. The post, camp, and station segment connects through the data center and provides access to the other network segments in both secure and nonsecure modes. The post, camp, and station segment allows users to train, collaborate, and conduct mission rehearsals. The installation processing node hosts enterprise services and applications associated with garrison operations. The installation processing node also connects users to installation-level services. The local NEC centrally manages these services. Applications and services within installation processing nodes provide either a temporary processing center presence until data center service is available or a permanent computing presence where technical or operational considerations dictate. The post, camp, and station segment supports major training exercises, such as mission readiness exercises and external evaluations. It also provides continuity of operations for the data center. NETCOM provides enterprise-level oversight and DODIN operations for the post, camp, and station network segment.

1-41. The deployed tactical network enables real-time employment of battle command common services, automated information systems, and information collection assets by deployed forces. The deployed tactical network enables the GCC and commander, joint task force (CJTF) to conduct joint, distributed operations with units in dispersed geographic locations. It allows commanders to conduct collective training with their units. The deployed tactical network connects to the DOD gateway to access DISN services, and to facilitate data replication at the data center for continuity of operations. This allows the unit to maintain its operational tempo with minimal mission impact. The tactical installation processing node hosts enterprise services and applications associated with operations while deployed. Figure 1-2 on page 1-9 depicts the DODIN-A.

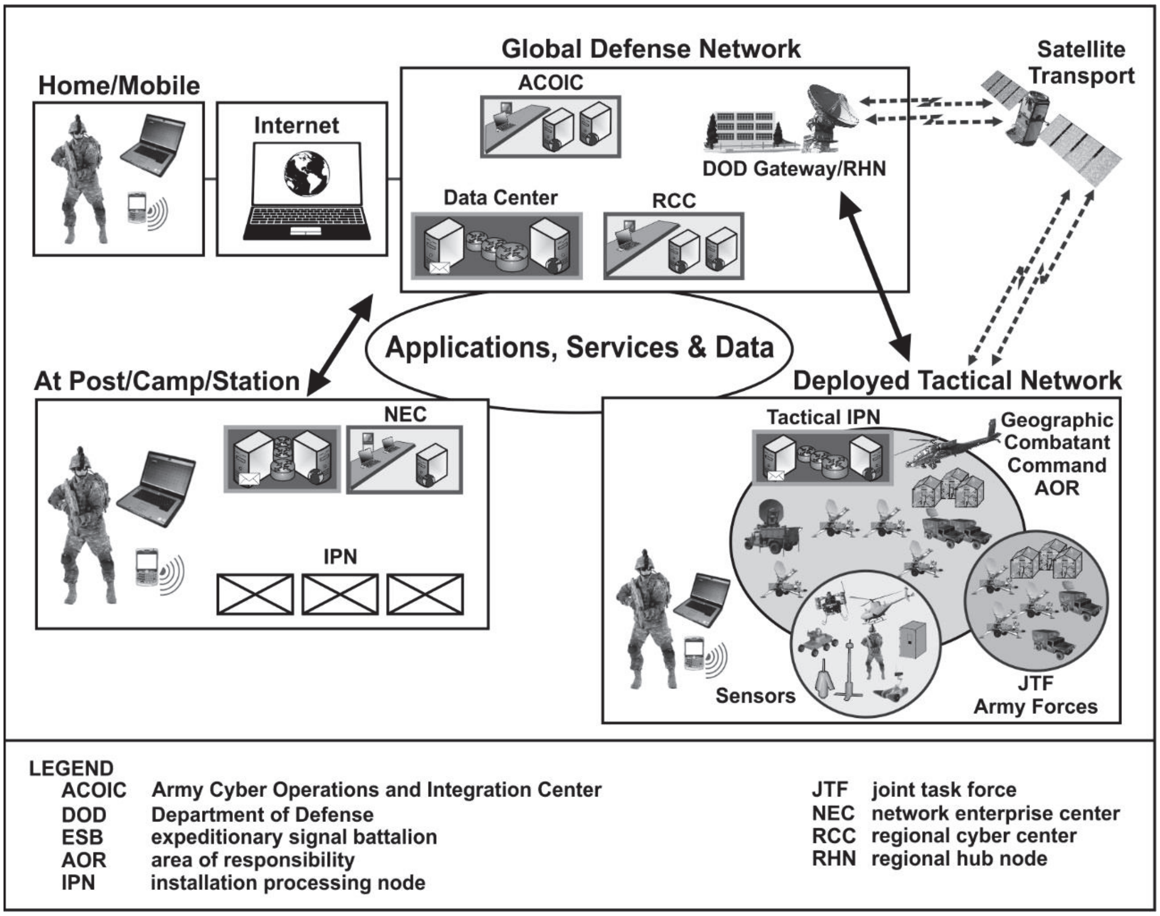

Global Defense Network
Satellite Transport
Home/Mobile
ACOIC
Internet
DOD Gateway/RHN
Data Center
RCC
Applications, Services & Data
At Post/Camp/Station
Deployed Tactical Network
NEC
Tactical IPN
Geographic Combatant Command AOR
IPN
Sensors
JTF Army Forces
LEGEND
ACOIC Army Cyber Operations and Integration Center
DOD Department of Defense
ESB expeditionary signal battalion
AOR area of responsibility
IPN installation processing node
JTF joint task force
NEC network enterprise center
RCC regional cyber center
RHN regional hub node

Figure 1-2. Department of Defense information network-Army

JOINT PHASES AND THE ARMY STRATEGIC ROLES

1-42. The joint force plans and conducts operations according to the six operational phases defined in the phasing model. During execution, a transition marks a change between phases or between the ongoing operations and execution of a branch or sequel. This shift in focus by the joint force is often accompanied by changes in command or support relationships and priorities of effort.

PHASING MODEL

1-43. Despite the numbering of the phases, the phasing model depicts the level of effort applied to each military activity, not necessarily a chronological sequence. While a large-scale combat operation may progress through all of the phases, most phase 0 shaping operations never transition to another phase. Phase IV stability operations or phase V operations to enable civil authority may also be standalone operations. A unit may deploy into an ongoing phase II, III, or IV operation directly from their home station without taking part in previous phases. See JP 3-0 and JP 5-0 for detailed information about the operational phases.

ARMY STRATEGIC ROLES

1-44. The Army accomplishes its mission by supporting the joint force in four strategic roles: shape operational environments, prevent conflict, conduct large-scale ground combat (win), and consolidate gains (FM 3-0). Strategic roles are not tasks assigned to subordinate units, but broad goals of an Army force. The Army conducts tactical tasks to accomplish each of its strategic roles to varying extents across each of the joint phases (see figure 1-3 on page 1-10). See FM 3-0 for more information about the Army's strategic roles.

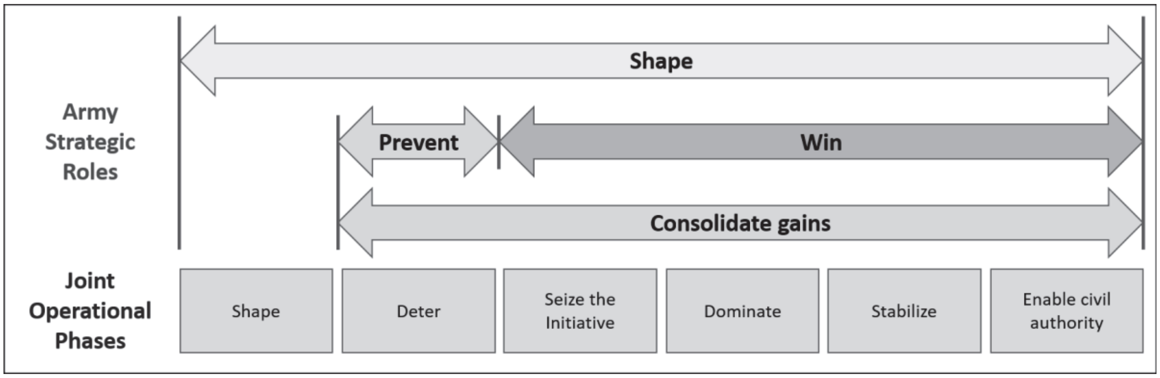
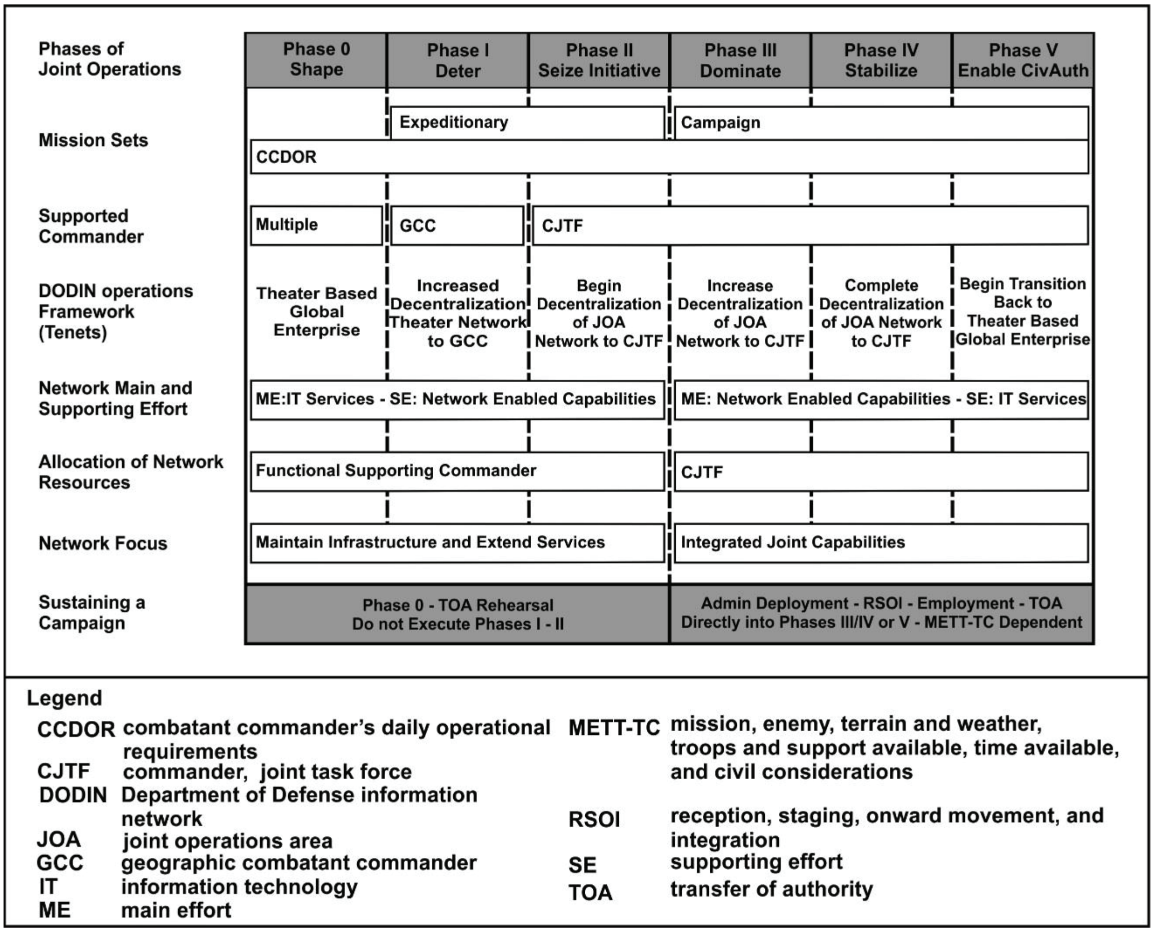


Figure 1-3. Army strategic roles' relationship to joint phases

DEPARTMENT OF DEFENSE INFORMATION OPERATIONS FRAMEWORK THROUGH THE OPERATIONAL PHASES

1-45. Theater DODIN operations roles, responsibilities, and relationships at the operational level shift as forces transition between phases. The DODIN operations framework adapts to the operational commander's requirements by phase. The framework indicates the DODIN operations priorities and support relationships across the joint operational phases. DODIN operations control and responsibilities shift as an operation matures and units arrive in the affected theater.

1-46. The mission and the level of development of the gaining command and theater dictate the actual transition of DODIN operations responsibilities. Units deploying into austere environments on contingency missions transition gradually until the gaining command is ready to accept them. Figure 1-4 on page 1-11 shows the transfer of DODIN operations authority as theater-focused operations progress through the phasing model.


Phases of Joint Operations
Phase 0 Shape
Phase I Deter
Phase II Seize Initiative
Phase III Dominate
Phase IV Stabilize
Phase V Enable CivAuth
Mission Sets
Expeditionary
Campaign
CCDOR
Supported Commander
Multiple
GCC
CJTF
DODIN operations Framework (Tenets)
Theater Based Global Enterprise
Increased Decentralization Theater Network to GCC
Begin Decentralization of JOA Network to CJTF
Increase Decentralization of JOA Network to CJTF
Complete Decentralization of JOA Network to CJTF
Begin Transition Back to Theater Based Global Enterprise
Network Main and Supporting Effort
ME:IT Services - SE: Network Enabled Capabilities
ME: Network Enabled Capabilities - SE: IT Services
Allocation of Network Resources
Functional Supporting Commander
CJTF
Network Focus
Maintain Infrastructure and Extend Services
Integrated Joint Capabilities
Sustaining a Campaign
Phase 0 - TOA Rehearsal Do not Execute Phases I - II
Admin Deployment - RSOI - Employment - TOA Directly into Phases III/IV or V - METT-TC Dependent
Legend

CCDOR	combatant commander’s daily operational requirements
CJTF	commander, joint task force
DODIN	Department of Defense information network
JOA	joint operations area
GCC	geographic combatant commander
IT	information technology
ME	main effort
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
RSOI	reception, staging, onward movement, and integration
SE	supporting effort
TOA	transfer of authority

Figure 1-4. Theater Department of Defense information network operations framework

PHASE 0—SHAPE

1-47. The purpose of shape phase missions, tasks, and actions is to dissuade or deter adversaries and assure friends, as well as set conditions for the contingency plan. Shaping missions are generally conducted through security cooperation activities. The shape phase generally aligns with the Army strategic role of shape. During the shape phase, the network is theater-focused. DODIN operations focus on meeting local commanders’ requirements. The priorities for network resource allocation support functional commands. The network’s main effort is access to IT services; the supporting effort is network-enabled capabilities. Units have daily access to automated information systems and maintain a SIPRNET presence for training and situational understanding. DODIN operations support the theater-focused global enterprise with priorities derived from the unit’s interaction with the strategic network. The mission sets support the generating force and the combatant commander’s daily operational requirements.

1-48. The regional hub node and data center connect units to the DODIN through both NIPRNET and SIPRNET and provides battle command common services to support mission command information systems. The RCC provides theater-wide DODIN operations oversight and situational awareness. Units have a single identity that follows them through all phases. The NEC administers this in the post, camp, and station network through a technique called installation as a docking station. Installation as a docking station connects tactical information systems to the DODIN-A through the installation campus area network. When operating on installation as a docking station, the unit performs all DODIN operations for its automated information systems as they would in a deployed tactical network, since the NEC has no visibility of these systems. Units can also disconnect from the installation campus area network and use their WIN-T equipment for training, employing the regional hub node to connect with DISN services.

PHASE I—DETER

1-49. The intent of this phase is to deter an adversary from undesirable actions because of friendly capabilities and the determination to use them. Deterrence leans toward security activities characterized by preparatory actions to protect friendly forces and indicate the intent to execute subsequent phases of the planned operation. In the deter phase, Army forces conduct tactical tasks to prevent conflict. In this phase, decentralization from a global enterprise to a theater network begins. Designated units receive warning orders, shifting their activities from the shape phase to the deter phase. The warning order triggers a series of actions that affect the DODIN and post, camp, and station network environments as the deployed tactical network takes shape. DODIN operations control begins to shift from the GCC to the CJTF as units rotate into the operational theater.

1-50. The DODIN-A and the other Services' network capabilities allow joint force commanders to package and examine available intelligence estimates in a crisis or on other indication of potential military action. The DODIN-A enables the tools and processes to focus intelligence efforts and refine estimates of enemy capabilities, dispositions, and intentions. These operational estimates allow staffs to develop courses of action within the context of the current situation and identify additional information requirements. Enterprise services facilitate planning and coordinating flexible deterrent options, and enable situational understanding and the command and control capabilities the GCC requires to resolve a crisis without armed conflict, or to deter further aggression.

1-51. During predeployment, the signal command (theater) [SC(T)] with DODIN operations responsibility for the deploying unit receives the warning order concurrently with the unit. The SC(T) prepares to transfer DODIN operations responsibility to the gaining theater as the unit progresses through the deployment process. The SC(T) alerts the signal brigade with regional responsibility for the unit. The signal brigade provides technical support to facilitate the unit's transition.

1-52. The network service center supports the deploying unit's transition to the gaining theater network during this phase. The network service center servicing the unit's home station coordinates to replicate necessary data and services to the gaining network service center and integrates the unit into the theater network infrastructure. The gaining theater's RCC assumes DODIN operations responsibility for the unit's automated information systems and aligns DODIN operations with the gaining commander's priorities. The unit continues predeployment training and takes part in a mission readiness exercise at a combat training center with their automated information systems integrated into the gaining theater network.

1-53. At this point, based on the situation, the GCC may have established a joint task force to conduct operations. The joint task force's joint network operations control center assumes DODIN operations responsibility when designated by the GCC.

1-54. Units deploying into the gaining theater provide the GCC with expeditionary capabilities—the ability to deploy combined arms forces quickly into an operational area and conduct operations upon arrival. The DODIN operations framework increasingly decentralizes to support the GCC. The network's main effort is providing IT services; the supporting effort is network-enabled capabilities. Network resource allocation supports the functional supporting commander's requirements. Units in this phase normally access DISN services using their organic network capabilities or a tailored, limited package from their organic capabilities. Commanders establish priorities of service to align the limited capabilities with their most critical mission requirements.

PHASE II—SEIZE INITIATIVE

1-55. Joint force commanders seek to seize the initiative in all situations through the decisive use of joint capabilities. In combat, this involves both defensive and offensive operations at the earliest possible time, forcing the enemy to culminate offensively and setting the conditions for decisive operations. During this phase, Army forces begin large-scale combat operations. By the time an operation reaches this phase, the unit conducts DODIN operations as part of the theater network. The unit has replicated all services and data to the gaining theater, disconnected from their post, camp, or station NEC and network service center, and deployed to the theater. The gaining network service center and supporting SC(T) verify the transfer of DODIN operations responsibility.

1-56. Upon arrival in the gaining theater, the unit aligns with its gaining command, reclaims its equipment, and coordinates with its DODIN operations authority. The gaining DODIN operations authority ensures the unit can access its replicated data and services and resolves issues integrating the unit into the theater network. Beginning with the seize initiative phase, the CJTF is the supported commander. The CJTF sets mission priorities and aligns DODIN operations to support these priorities. DODIN operations responsibility and authority transition from the GCC to the CJTF as they posture the joint task force. In this phase, expeditionary units receive their network support using their organic signal assets connecting to the DODIN through the regional hub node.

Phase III—Dominate

1-57. This phase focuses on breaking the enemy's will to resist or, in noncombat situations, controlling the operational environment. Success in the dominate phase depends on overmatching enemy capabilities at the critical time and place. The network's primary focus is supporting the CJTF, who establishes mission priorities that may change over the course of operations. DODIN operations align to meet and support these priorities and adapt to mission changes. The deployed tactical network is a joint network over which the CJTF exercises DODIN operations control.

1-58. The CJTF is the supported commander beginning with the dominate phase. The mission sets are campaign-oriented. The network main effort is network-enabled capabilities to support these mission sets. The supporting effort is IT services. The GCC allocates network resources to the CJTF. The CJTF uses the network to integrate joint capabilities. The CJTF continues to control the network for the rest of the phases. As larger force packages enter the theater, signal support units deploy to augment the theater portion of the network and establish more robust network infrastructure on forward operating bases.

Phase IV—Stabilize

1-59. Forces enter the stabilize phase as they shift from sustained combat operations to stability activities. The CJTF still exercises DODIN operations control of the network. DODIN operations remain aligned to joint task force mission priorities, with responsibilities delegated according to the DODIN operations framework. In this phase, Army forces focus their efforts on consolidation of gains.

Phase V—Enable Civil Authority

1-60. This phase primarily consists of joint force support to legitimate civil governance. The desired end state is terminating operations and redeploying the joint forces. In this phase, the network reverts to theater-focused to meet local commanders' information requirements. Redeploying units reverse the transition from the earlier phases, return to their home stations, and reintegrate into their post, camp, and station networks. In this phase, Army forces continue to consolidate gains until the transition to legitimate authorities.

This page intentionally left blank.

Chapter 2

Department of Defense Information Network Operations Roles and Responsibilities

DODIN operations ensure users' network and information systems connectivity and security throughout the DODIN. This chapter explains the distributed roles and responsibilities of DODIN operations entities and network managers from the global, strategic level to the theater army, corps, division, and brigade. It further identifies and describes the control centers that perform DODIN operations functions to manage, control, and secure tactical networks, and their interfaces into the DODIN.

SECTION I – GLOBAL LEVEL

UNITED STATES CYBER COMMAND

2-1. United States Cyber Command (USCYBERCOM) has the sole authority and responsibility to secure, operate, and defend the DODIN. In this capacity, USCYBERCOM carries out operational and tactical level planning and day-to-day management responsibilities for DODIN operations and defense. Combatant commanders coordinate through USCYBERCOM to consider global impacts to the DODIN. USCYBERCOM plans, coordinates, integrates, and synchronizes activities to direct DODIN operations and defense, and conducts offensive cyberspace operations when directed. See JP 3-12 for information on offensive cyberspace operations.

2-2. The USCYBERCOM Joint Operations Center performs crisis planning, synchronization, direction, and execution of current cyberspace operations. The USCYBERCOM Joint Operations Center—

- Directs DODIN operations and defense.
- Develops processes and policies to enable comprehensive cyberspace situational understanding.
- Establishes partnerships to develop network defense tools.
- Centralizes operation and maintenance of cross domain solutions.
- Analyzes cyberspace risk.
- Develops and recommends countermeasures to events.
- Executes continuity of operations.

DEFENSE INFORMATION SYSTEMS AGENCY

2-3. The Defense Information Systems Agency is a combat support agency of the DOD. The agency provides, operates, and ensures information sharing capabilities and a globally accessible enterprise information infrastructure to support joint warfighters, national-level leaders, and joint, inter-organizational, and multinational elements across the range of military operations. The Director, Defense Information Systems Agency reports to the DOD Chief Information Officer.

2-4. The Director, Defense Information Systems Agency has dual responsibilities as Commander, Joint Force Headquarters-DODIN under the operational control (OPCON) of USCYBERCOM. Joint Force Headquarters-DODIN provides operational-level network command and control to direct and verify the DODIN's defensive posture. Joint Force Headquarters-DODIN exercises tactical control of the Service cyber components and supports the geographic combatant commands to synchronize global and theater DODIN operations. Joint Force Headquarters-DODIN exercises directive authority to ensure all Services, combatant commands, agencies, and field activities actively implement the security measures necessary to secure their portions of the DODIN and minimize shared risk.

2-5. Joint Force Headquarters-DODIN does not duplicate the DODIN operations activities performed by the Services and defense agencies. It engages to perform—

- Activities specifically directed by USCYBERCOM.
- DODIN operations activities the Service components and agencies cannot perform.
- DODIN operations activities more effectively executed at the joint level.

CHIEF INFORMATION OFFICER/G-6

2-6. The Chief Information Officer (CIO)/Assistant Chief of Staff, Signal (G-6) establishes policy for Army use of information technology systems and networks. This responsibility includes evaluating existing Army information management and information technology policies and overseeing their implementation. The CIO/G-6 sets the strategic direction for, and supervises the implementation of, Army information management programs and policy. These programs and policies include network architecture, information sharing policy, cybersecurity policy, the Army cybersecurity program, resource management, process modernization, and synchronization of the Army's network activities.

UNITED STATES ARMY CYBER COMMAND

2-7. United States Army Cyber Command (ARCYBER) is an Army Service component command to USCYBERCOM. ARCYBER is the primary Army headquarters responsible for cyberspace operations to support joint requirements. ARCYBER is the single point of contact for reporting and assessing cyber incidents, events, and operations in Army networks, and for synchronizing and integrating Army responses. When directed, ARCYBER conducts offensive and defensive cyberspace operations to ensure U.S. and allied freedom of action in cyberspace, and to deny the same to adversaries. ARCYBER provides appropriate-level interactions both as a supported and as a supporting commander to other Army Service component commands (including theater armies), Army commands, direct reporting units, and joint, inter-organizational, and multinational elements.

2-8. Commander, USCYBERCOM has designated the ARCYBER commander as the Commander, Joint Force Headquarters-Cyber to provide command and control of joint and coalition cyberspace forces. See JP 3-12 for information on joint cyberspace operations. Figure 2-1 on page 2-3 illustrates ARCYBER's structure and DODIN operations relationships.

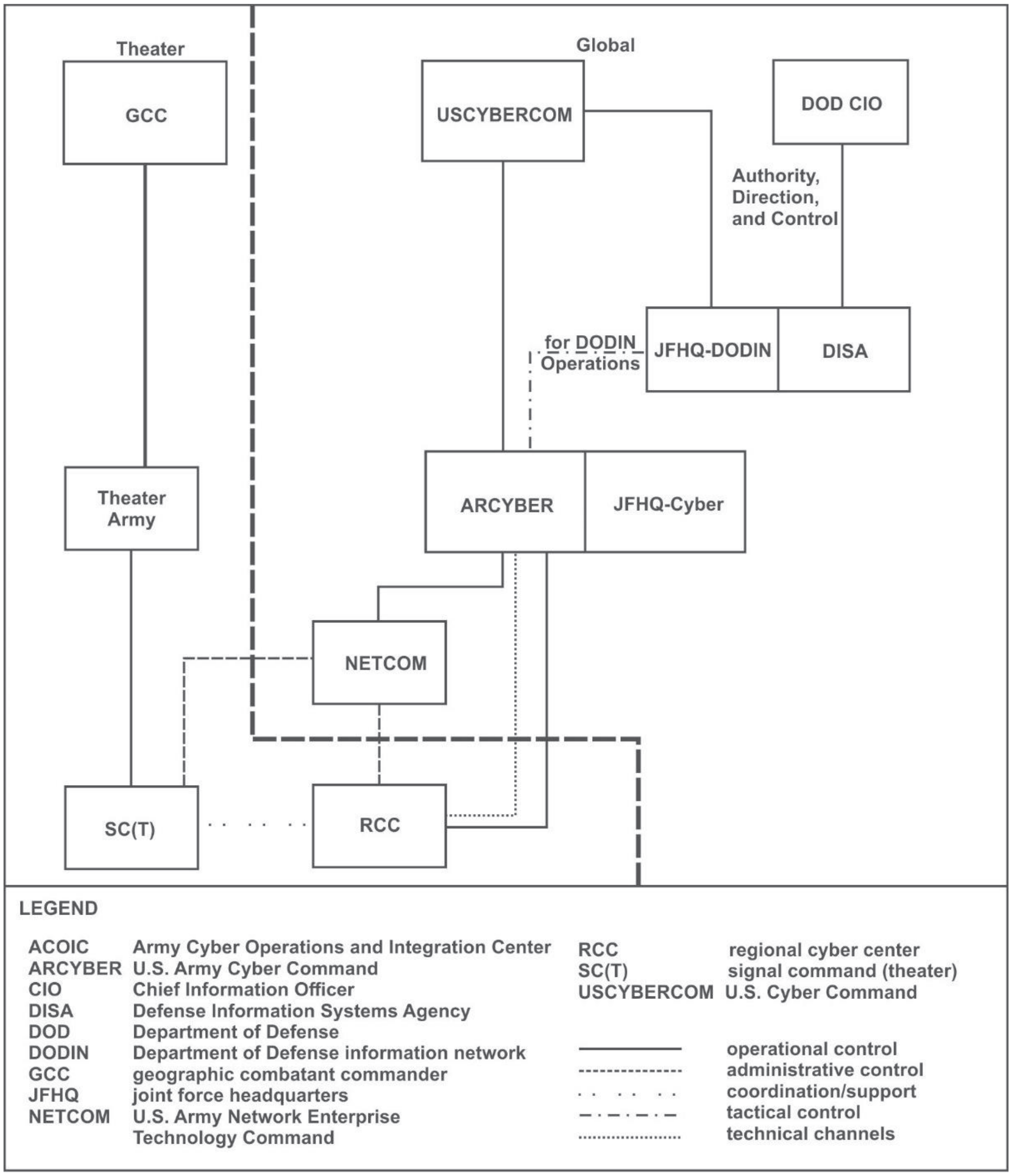

Theater
Global
GCC
USCYBERCOM
DOD CIO
Authority, Direction, and Control
for DODIN Operations
JFHQ-DODIN
DISA
Theater Army
ARCYBER
JFHQ-Cyber
NETCOM
SC(T)
RCC
LEGEND
ACOIC Army Cyber Operations and Integration Center
ARCYBER U.S. Army Cyber Command
CIO Chief Information Officer
DISA Defense Information Systems Agency
DOD Department of Defense
DODIN Department of Defense information network
GCC geographic combatant commander
JFHQ joint force headquarters
NETCOM U.S. Army Network Enterprise Technology Command
RCC regional cyber center
SC(T) signal command (theater)
USCYBERCOM U.S. Cyber Command
operational control
administrative control
coordination/support
tactical control
technical channels

Figure 2-1. United States Army Cyber Command Department of Defense information network operations relationships

1ST INFORMATION OPERATIONS COMMAND

2-9. The 1st Information Operations Command is under OPCON of ARCYBER and administrative control of United States Army Intelligence and Security Command. It provides information operations planning, intelligence, and training support to Army forces and other Services.

UNITED STATES ARMY NETWORK ENTERPRISE TECHNOLOGY COMMAND

2-10. NETCOM engineers, installs, operates, maintains, and secures the DODIN-A to enable command and control and support the other warfighting functions through all Army operations and missions. NETCOM is the Army's global enterprise network service provider and performs DODIN operations on behalf of

ARCYBER to gain information advantage. NETCOM's standardized DODIN operations ensure interoperability in a joint, inter-organizational, and multinational enterprise network.

2-11. NETCOM is the authorizing official for the Army enterprise, as directed by the Department of the Army CIO/G-6. NETCOM integrates Army IT to achieve a single, virtual enterprise network by overseeing end-to-end management of the Army enterprise service area, including 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 Army networks and functional processing centers. To ensure unity of effort in DODIN operations, NETCOM has direct liaison authority to the Chief Information Officer/G-6, with notification to ARCYBER.

2-12. NETCOM manages the DODIN-A, including enforcing cybersecurity, technical, and configuration management programs and policies according to AR 25-1 and AR 25-2. NETCOM is the single entry point to submit validated telecommunications requirements to the Defense Information Systems Agency for coordination and implementation.

GLOBAL DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS ORGANIZATIONS

2-13. The DODIN operations architecture focuses on central management from higher-level echelons and decentralized execution. Within the DODIN, many organizations perform network and information systems management, cybersecurity, and physical and operational management functions. These organizations manage the DODIN through an established hierarchy of DODIN operations control centers. To ensure worldwide interoperability of the network and reduce redundant efforts, some DODIN operations activities take place at the global level. Global oversight also allows holistic network situational understanding. These control centers integrate DODIN operations to support communications and information systems. USCYBERCOM, joint and combatant commands, and Service components operate and manage these centers to control their respective portions of the DODIN. DODIN operations facilities at every level should be prepared to assume the responsibilities and functions of the next higher, lower, and adjacent DODIN operations elements in case of catastrophic failure, for example, battle damage, terrorist attack, or natural disaster.

ARMY CYBER OPERATIONS AND INTEGRATION CENTER

2-14. The ACOIC is an operational element of the ARCYBER headquarters. The ACOIC is the top-level control center for all Army cyberspace activities. The ACOIC provides DODIN operations reporting for Army networks and the wider DODIN, and situational understanding for Army networks. The ACOIC also provides worldwide operational and technical support for the DODIN-A across the strategic, operational, and tactical levels, in coordination with the theater armies. The ACOIC interfaces with the RCC, functional NOSCs, and other Service and agency DODIN operations centers.

2-15. The ACOIC analyzes threat information and directs network security actions to the RCCs in coordination with the theater armies. The ACOIC develops technical solutions to secure Army networks, and helps subordinate units implement network security measures.

ARMY ENTERPRISE SERVICE DESK

2-16. The Army Enterprise Service Desk provides user support to Army IT customers. The Army Enterprise Service Desk is the central agent for tier 0 and tier 1 service and application support.

2-17. The Army Enterprise Service Desk delivers a consistent set of centralized service desk processes to reduce manpower requirements. It uses cost effective assets and aligns with the Army's strategic vision. Army Enterprise Service Desk responsibilities include—

- Detecting incidents or reports of incidents.
- Accepting incident assignments.
- Performing initial diagnosis of an incident.

- Validating assignment of an incident.
- Troubleshooting an incident.
- Determining if incident functional escalation is required.
- Determining if hierarchical escalation is required.
- Escalating incidents as required.
- Reassigning an incident internally to another cyber center support group.
- Taking corrective actions to restore service.
- Performing incident resolution.
- Participating in post incident reviews.
- Performing process overview and review.
- Recommending process changes to the process lead.

Functional Network Operations and Security Centers

2-18. A functional NOSC performs the same enterprise manager functions as an RCC (see paragraph 2-54). While the RCCs' operational areas align with a geographic location, the functional NOSCs responsibilities align with a function, such as Army National Guard or special operations.

2-19. The Army National Guard operates a functional NOSC that provides the RCC functions for the states and territories, and administers GuardNet. The Army National Guard Information Networks Division manages GuardNet as an enterprise network that connects all the state and territory intranets.

2-20. The special operations signal battalion operates a functional NOSC to support the Army special operations forces communications system in a theater. See ATP 3-05.60 for more information about the Army special operations communications system.

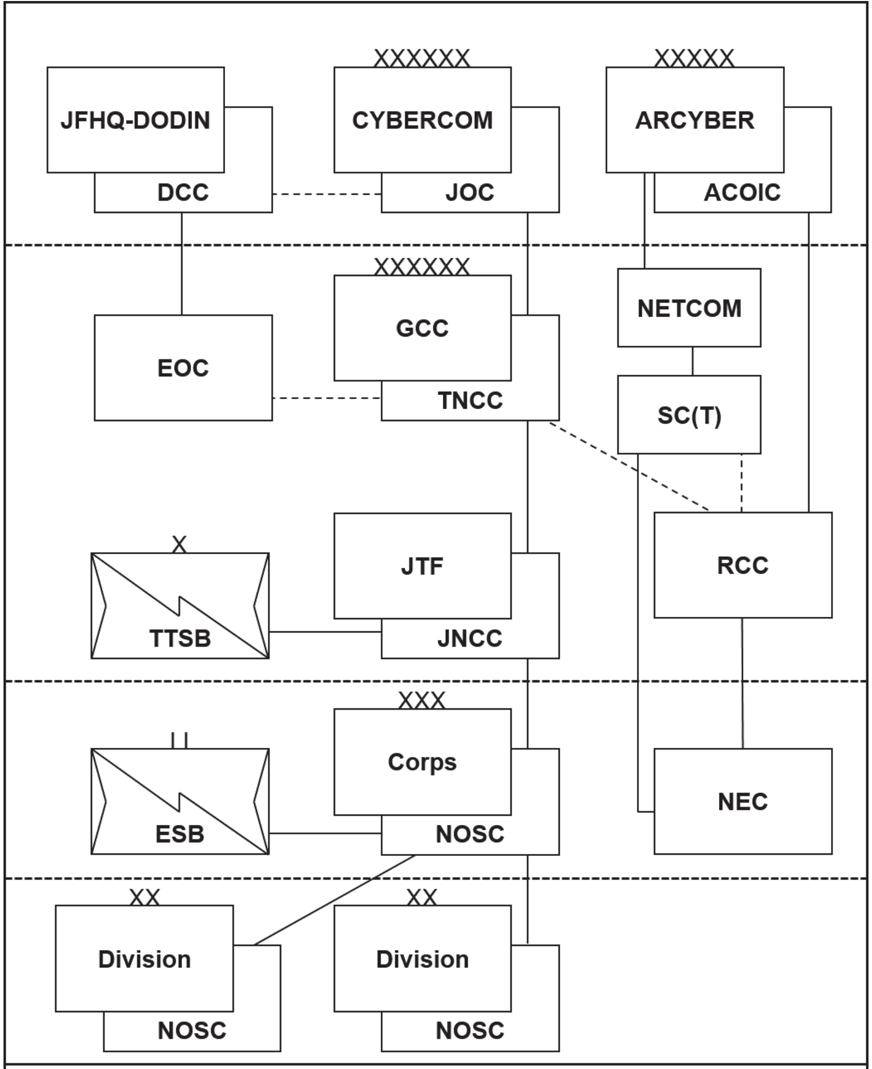
SECTION II – THEATER LEVEL

2-21. From an operational perspective, the theater network consists of that portion operated by a GCC, its sub-unified and component commands, its joint and single-Service task forces, and installations and activities within the AOR. From a technical perspective, it is a subset of DODIN assets, resources, and services supporting that theater.

2-22. The GCCs direct joint DODIN operations in their respective theaters with support from Commander, USCYBERCOM, the USCYBERCOM Joint Operations Center, and the SC(T) associated with the theater army. The Defense Information Systems Agency provides an enterprise operations center for each theater under the tactical control of the GCC. Each GCC also has a theater network operations control center (TNCC) to maintain network situational understanding and provide operational and tactical control of their respective systems and network. Comprehensive network situational awareness allows commanders to make informed decisions to align network assets and capabilities to mission priorities and secure the network.

2-23. The joint cyberspace center (JCC) and TNCC collaborate with the USCYBERCOM cyberspace support element, the Defense Information Systems Agency enterprise operations center, and Service component DODIN operations centers, as appropriate, to ensure effective operation and defense of the DODIN in the theater. The enterprise operations center also offers onsite support teams for the theater. The enterprise operations center develops, monitors, and maintains the theater network situational awareness view. The geographic combatant command communications system directorate of a joint staff (J-6) provide requirements to aggregate and segment the theater network situational awareness view, as derived from the DODIN common network management data exchange standards (see DODI 8410.03). The network situational awareness view includes operational and tactical enterprise management, cybersecurity, and content management status. The enterprise operations center coordinates reporting requirements and the network situational awareness view with the JCC and TNCC.

2-24. The GCC exercises OPCON over all assigned DODIN operations elements and the theater network. The enterprise operations center is under the tactical control of the GCC for DODIN operations in the theater. The TNCC operates the theater network. The TNCC coordinates with the enterprise operations center and directs the Service component DODIN operations organizations to ensure the theater network supports the mission. The USCYBERCOM Joint Operations Center may provide support to ensure the theater network supports the GCC's requirements. Figure 2-2 depicts a notional theater DODIN operations structure.



LEGEND

ACOIC	Army Cyber Operations and Integration Center
ARCYBER	United States Army Cyber Command
CYBERCOM	United States Cyber Command
DCC	Defense Information Systems Agency
DODIN	Command Center
EOC	Department of Defense information network
ESB	enterprise operations center
GCC	expeditionary signal battalion
JFHQ	geographic combatant commander
JNCC	joint force headquarters
JOC	joint network operations control center
JTF	joint operations center
NOSC	joint task force
RCC	network operations center
SC(T)	regional cyber center
TNCC	signal command (theater)
	theater network operations control center
- - - - - - -	coordinating authority
———	technical channels

Figure 2-2. Theater Department of Defense information network operations structure

2-25. USCYBERCOM adjudicates conflicts or resource contentions that arise due to a GCC's requirements. USCYBERCOM forwards conflicts they cannot resolve to the Chairman of the Joint Chiefs of Staff for adjudication. Services and agencies may establish theater-level operations centers or provide an uninterrupted theater-level network situational awareness view to support the GCCs' and their Service components' requirements. The global or theater operations center provides theater network visibility to the enterprise operations center and DOD component operations centers, as required. This Service or agency DODIN operations center also serves as the central point of contact for operational matters and emergency provisioning for a supported GCC to improve network situational understanding at all levels of command and enable end-to-end management of the DODIN.

GEOGRAPHIC COMBATANT COMMANDER

2-26. The GCC exercises combatant command authority over the Service and functional component commands in theater. The GCC exercises OPCON over all signal forces and associated DODIN operations elements within their AOR. This responsibility includes organizations and systems the DOD Services and agencies provide to extend the DODIN into the theater. The GCC's supporting DODIN operations organizations manage the theater network situational understanding data stores, databases, and graphical views. The GCC establishes information collection, filtering, display, and dissemination priorities. The GCC controls release of theater network status information to supporting and multinational forces, consistent with these priorities. The GCC aggregates theater network event, performance, and fault reporting data from subordinate and supporting Service and functional component commands and joint task forces relating to all systems and networks within their AOR to develop the network situational awareness view.

COMBATANT COMMAND J-6

2-27. The J-6 establishes policy and guidance for all communications assets supporting the joint force commander, and develops communications system architectures and plans to support the GCC's mission. The J-6 also advises the GCC of the network's ability to support operations.

2-28. The J-6 develops policy and guidance for integrating and configuring operational networks and controls the joint information systems infrastructure. The J-6 exercises staff supervision and controls theater assets that the Defense Information Systems Agency, other Services, and other DOD agencies provide. The J-6 oversees theater DODIN operations through technical channels. ***Technical channels*** **are the chain of authority for ensuring the execution of clearly delineated technical tasks, functions, and capabilities to meet the dynamic requirements of Department of Defense information network operations.**

2-29. Awareness of all current, future, or contemplated DODIN operations allows the JCC to advise the GCC of the network's ability to support assigned missions and operations. Maintaining situational awareness requires continual coordination with the USCYBERCOM cyberspace support element, the Defense Information Systems Agency, and the Defense Intelligence Agency.

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

JOINT CYBERSPACE CENTER

2-30. The JCC is the operational element of the combatant command that integrates DODIN operations, defensive cyberspace operations, and offensive cyberspace operations in the theater. As an operational extension of the GCC's command center, the JCC provides the commander and the enterprise operations center with the theater network situational awareness view and operational impact assessments. For more information about the JCC's defensive and offensive cyberspace operations roles, see JP 3-12.

2-31. In coordination with the TNCC, the JCC establishes the network situational awareness view based on commander and J-6 guidance and subordinate commands' requirements. The commander decides the minimum status information to ensure consistent, common situational understanding. Standardizing the status information simplifies integrated and roll-up views generated by different theaters or organizations.

Theater Network Operations Control Center

2-32. The TNCC controls all theater systems and networks operated by forces assigned to or supporting the GCC through technical channels. The TNCC, in coordination with the JCC, responds to USCYBERCOM direction for global DODIN operations issues. The TNCC's roles include—

- Monitoring the theater network.
- Determining operational impact of degradations and outages.
- Coordinating responses to degradations and outages that affect joint operations.
- Coordinating network actions to support changing operational priorities.

2-33. The TNCC aggregates the network situational awareness view from the enterprise operations center, Service component DODIN operations organizations, and joint network operations control center. Shared network situational understanding enables the success of the GCC's missions. The network situational awareness view application is part of an enterprise-wide software toolset, but the input data requirements and output reports are user-definable to meet each commander's needs.

2-34. The TNCC prioritizes and directs operational actions through the supporting enterprise operations center and DODIN operations personnel. The TNCC directs system and network management activities throughout the theater to support the GCC's DODIN operations decisions. To carry out its mission, the TNCC—

- Collaborates with the DODIN operations community of interest to ensure effective DODIN operation and defense.
- Tracks system and network outages and customer service shortfalls.
- Consolidates and analyzes reports from Service components, agencies, joint task forces, and deployed units.
- Directs DODIN operations event reporting, analyzes the impact of events on the operational mission, develops alternate courses of action, and advises the commander and other senior decision makers on the status of network degradations, outages, events, and areas requiring improvement.
- Establishes priorities for installing, configuring, and restoring systems and network services for the enterprise operations center and subordinate organizations.
- Directs, coordinates, and integrates response to network attacks and intrusions affecting the theater network.
- Directs the theater response to USCYBERCOM directives for global DODIN operations issues.
- Coordinates with USCYBERCOM to reconcile the GCC's DODIN operations priorities with the global priorities.

ENTERPRISE OPERATIONS CENTER

2-35. The Defense Information Systems Agency operates the enterprise operations center to provide near real-time monitoring, coordination, control, and management of the theater network. The enterprise operations center aggregates and disseminates the consolidated network situational awareness view in a combatant command AOR. This capability includes shareable, look-up and lookdown views of Service component and joint task force elements in the theater.

2-36. The enterprise operations center develops, monitors, and maintains the network situational awareness view based on GCC or global enterprise operations center requirements. The situational awareness view includes pertinent theater, operational, and tactical system, network, and content management status information. To carry out its mission, the enterprise operations center—

- Operates and maintains the DISN backbone services in their theater.
- Coordinates theater network support, in collaboration with the TNCC.

- Collaborates with the DODIN operations community of interest to ensure effective operation and defense of the DODIN.
- Issues technical directives to Service DODIN operations centers to ensure compliance with GCC and USCYBERCOM direction.
- Supports the GCC, Services, and agencies by creating and disseminating the theater network situational awareness view. The network situational awareness view includes wireless and terrestrial links, satellite communications systems, and enterprise services.
- Maintains situational understanding to support current and near-term operations and deliberate plans.
- Coordinates reporting requirements and view specifications for network situational understanding with the JCC and TNCC.
- Continuously monitors and collects performance data for information resources based on GCC and global enterprise operations center priorities.
- Provides information security services to the TNCC or global enterprise operations center, including—
  - Monitoring, reporting, and analysis of intrusions and physical threats.
  - Correlating intrusion incidents with Service components, sub-combatant commands, and joint task forces.
- Helps identify the mission effects of degradations, outages, and DODIN events.
- Identifies and resolves security anomalies affecting theater network assets.
- Performs incident and intrusion monitoring and detection, strategic vulnerability analysis, computer forensics, and theater network-related activity response.
- Identifies courses of action and directs restoration of capabilities and services, when required.
- Directs courses of action and coordinates incident response to secure networks under attack.
- Coordinates with, and receives support from, the law enforcement and counterintelligence center.
- Manages theater radio frequency interference resolution.
- Supports satellite anomaly resolution.
- Supports satellite communications interference resolution.

JOINT TASK FORCE

2-37. If a theater army, corps, or division is the designated joint task force headquarters, its G-6 usually becomes the joint task force J-6. If another Service is the designated joint task force headquarters, Army G-6s function as subordinate organizations to the joint task force J-6. The CJTF controls joint force systems and networks through a joint network operations control center. Refer to JP 3-33 for more information on joint task force operations.

THEATER ARMY G-6

2-38. Theater army signal support consists of the theater army G-6 staff and the SC(T). The SC(T) commander may also act as the theater army G-6. The G-6 is the principal advisor to the theater army commander on information management and information system matters across the AOR. The G-6 staff focuses on Army requirements in the theater.

2-39. The G-6 staff plans, manages, and controls communications systems input, information systems architecture, and long-range modernization plans for the theater army. It manages network enterprise initiatives and ensures the theater network architecture complies with DOD and Army standards.

SIGNAL COMMAND (THEATER)

2-40. The SC(T) provides DODIN operations capabilities to support Army, joint, and multinational forces in theater through its associated RCC. These capabilities use the DODIN-A for network extension and reachback to support the GCC. In coordination with the RCC, the SC(T) operates Army networks in the theater and delivers common user services to support the GCC and the theater army. With joint augmentation, the SC(T) may also assume joint or multinational DODIN operations responsibility for a joint task force. As the theater's senior Army signal commander, the SC(T) commander may be designated to serve as the J-6 of an Army-led joint task force, or the Army forces (ARFOR) G-6.

2-41. The theater army may task the SC(T) to provide overall control of theater signal assets. All or a portion of the SC(T) may be tasked to establish or augment the joint network operations control center, or provide land forces network control when tasked as part of an ARFOR. The SC(T) is comprised of a headquarters and one or more theater strategic signal brigades. The SC(T) DODIN operations responsibilities include—

- Providing centralized management and control for the theater army's data, voice, and video networks, including interfaces with joint, combined, and multinational systems via the RCC.
- Facilitating or establishing the joint network operations control center to support the CJTF.
- Enforcing cybersecurity policies and directions to support the GCC and theater army commander.
- Tailoring Army signal support to meet operational requirements.
- Providing direct support to Army signal formations supporting the ARFOR and joint task force.
- Providing guidance and governance through technical channels to Army NOSCs within the theater.
- Supervising DODIN operations tool employment.
- Providing DODIN operations and operational management for network and automation assets provided by external organizations and agencies according to applicable service level agreements.
- Ensuring the cybersecurity tools are in place to maintain the integrity of the network, and to support secure access controls and connectivity.
- Implementing plans, policies, and procedures to install, operate, maintain, and secure assigned portions of the DODIN.
- Establishing, or augmenting and staffing the Army's portion of, the joint network operations control center, as required.
- Conducting spectrum management operations for Army, joint, and multinational elements throughout the theater. *Spectrum management operations* are the interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations (FM 6-02).
- Validating satellite communications requirements and managing ground mobile force tactical satellite communications equipment in the theater.

Note. In a theater with no assigned SC(T), the strategic signal brigade commander and staff carry out these functions as the senior signal organization in theater.

THEATER TACTICAL SIGNAL BRIGADE

2-42. The theater tactical signal brigade provides command and control and staff supervision for its subordinate expeditionary signal battalions, expeditionary signal companies, and joint/area signal companies. The brigade staff develops local area network and wide-area network (WAN) architectures necessary to accomplish the brigade's current and future missions. The brigade staff oversees the installation, operation, and maintenance of tactical communications systems by their subordinate battalions and companies.

2-43. The theater tactical signal brigade staff may also reinforce the supported G-6's DODIN operations. The supported G-6 makes network and augmentation requirement recommendations to the commander for effective DODIN operations. Augmenting the supported G-6 is situation-dependent, and requires close coordination between maneuver commanders, G-6s, and signal unit commanders to ensure the theater tactical signal brigade provides the necessary personnel and equipment to support the mission. When elements of the theater tactical signal brigade support a unit with an organic NOSC capability, they configure their systems to report status to the supported unit NOSC. When theater tactical signal brigade elements support a unit with no DODIN operations capability, they configure their systems to report status to the RCC through the regional hub node or DOD gateway. Refer to FM 6-02 for more information on the theater tactical signal brigade and supporting units.

STRATEGIC SIGNAL BRIGADE

2-44. The strategic signal brigade provides the fixed theater communications infrastructure and services. Each strategic signal brigade is unique and tailored to support theater-specific communications infrastructure requirements. The RCC supports the strategic signal brigade in performing DODIN operations for theater networks and information systems. These functions include backbone networks, e-mail, spectrum management, communications circuitry, gateway routing to multinational networks, commercial telephone access in theater, and Defense Switched Network access to outside of the theater. The strategic signal brigade provides NEC services and support throughout its area of operations using its organic signal battalions, companies, and detachments.

THEATER DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS ORGANIZATIONS

2-45. An interoperable theater network enables unity of command and unity of effort within a geographic AOR, as well as between AORs. Theater-level DODIN operations help joint force commanders exercise their DODIN authorities in their AOR.

NETWORK SERVICE CENTER

2-46. The overarching technique for implementing the Army enterprise network is the employment of the network service center. The network service center integrates three critical components—

- **Enterprise manager (RCC)**—provides DODIN operations oversight for Army forces in theater.
- **Regional hub node**—extends DODIN access and reachback to deployed units.
- **Data center**—provides enterprise IT services, application hosting, and backup for mission command, intelligence, and business systems.

2-47. Network service centers implement standardized policies to integrate voice, data, imagery, and DODIN operations capabilities, down to Soldier level, across all echelons. The network service center is not a facility, but a logical collection of capabilities (see figure 1-1 on page 1-5). The network service center enhances the Army's ability to—

- Maintain a continental United States-based Army that deploys to, and operates successfully in, remote operational areas.
- Rapidly and dynamically task-organize to enable operational flexibility.
- Train as it fights.
- Fight on arrival.

Enterprise Manager

2-48. The enterprise manager is the Army's lead DODIN operations authority throughout their service area. Enterprise managers' service areas are defined either geographically (the RCC) or functionally (Army National Guard NOSC or special operations forces NOSC).

Regional Hub Node

2-49. The *regional hub node* is a component of the network service center, which provides a transport connection between the Warfighter Information Network-Tactical and the wider Department of Defense information network (ATP 6-02.60). The regional hub node's network transport extends DISN services to deployed WIN-T enabled units. Network transport is the processes, equipment, and transmission media that provide connectivity and move data between networking devices and facilities. NETCOM maintains a limited amount of leased commercial satellite bandwidth for the regional hub nodes to support contingencies. Regional hub nodes provide the primary communications hub capability for operational forces.

2-50. A typical regional hub node can support up to 3 Army divisions and 12 separate enclaves, such as a brigade combat team (BCT), support brigade, or joint user, or up to 56 discrete missions simultaneously. Regional hub nodes' geographic distribution provides global coverage. Regional hub nodes are located at DOD gateway sites to provide a connection to DISN services. See ATP 6-02.60 for more information on the regional hub node.

Data Center

2-51. The data center is the Army's DODIN operations element that provides the primary information services capability within the enterprise, relaying SIPRNET and NIPRNET services within all theaters. Data centers deliver standardized local, regional, and global network services from centrally managed locations. The data center concentrates interconnectivity, hosts common servers and services, and interfaces users with the DODIN-A through an enhanced security gateway. Data centers improve the Army's DODIN operations posture by reducing the number of access points into the DODIN-A and by employing standardized DODIN operations tools and processes.

2-52. An installation processing node is a fixed data center serving a single DOD installation and its local area. It provides local services that a DOD core data center cannot technically or economically provide. There is no more than one installation processing node per installation, but an installation processing node may have multiple enclaves to accommodate unique installation needs, such as joint bases.

2-53. The installation security router forms the boundary of the installation processing node. The installation security router is the security perimeter to the local processing center that houses applications and servers, and the interface to the installation's local area networks.

Data Center Consolidation

2-54. Army systems and networks face the constant risk of compromise and disruption. Each IT system and application presents a potential attack surface for enemies and adversaries. For this reason, the Army is reducing the number of Army IT systems and applications and optimizing those remaining to operate in modern, cloud-enabled computing environments. The Army is consolidating its data centers to one installation processing node for each post, camp, or station as part of the larger DOD goal to reduce data center infrastructure by at least 60 percent. Reducing the number of data centers will enable transition to the long-term end state of four Army enterprise data centers in the continental United States and six outside the continental United States.

Regional Top Level Architecture (Joint Regional Security Stack)

2-55. A top level architecture provides perimeter protection in the distributed DOD network. Joint information environment is replacing over 1,000 installation-based top level architectures across the DOD with fewer than 50 regional top level architectures (joint regional security stacks). Reducing the number of top level architectures minimizes the DODIN's threat surface and cybersecurity workload. In the Army's consolidated security architecture, the post, camp, or station network perimeter logically extends to the joint regional security stack hosted at a DOD core data center, defense enterprise computing center, or at a Service base, post, camp, or station. The installation processing node and the joint regional security stack support defense-in-depth. *Defense-in-depth* is an information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization (CNSSI 4009). The installation processing node provides perimeter protection for the local processing center at selected posts, camps, and stations according to security technical implementation guides (see paragraph 3-62) and isolates the Army intranet from external traffic on a post, camp, or station.

> ***Note.*** On full implementation of the joint information environment, the Army will eliminate all installation-based top level architectures.

REGIONAL CYBER CENTER

2-56. The RCC is the single DODIN operations point of contact in the theater for Army network services, operational status, service provisioning, and service interruption resolution and restoral. The RCC provides network visibility and status information to the Defense Information Systems Agency enterprise operations center in theater. In some theaters, the RCC provides network visibility to other Service component DODIN operations centers. RCCs perform the same functions and use the same tactics, techniques, and procedures across all theaters.

2-57. While all units are responsible for securing their respective portions of the network, the RCC exercises overall responsibility for securing the Army's portion of the theater network. The RCC develops technical solutions to ensure network security, and helps subordinate units implement network security. The RCC helps develop theater cybersecurity policy and implements that policy.

2-58. The RCC performs or coordinates DODIN operations tasks that span the theater or multiple regions to provide consistent service among regions. This places the operational function at the only location in the theater with visibility or awareness of multiple regions. The RCC's DODIN operations responsibilities include—

- Providing event and incident management capabilities, such as analysis and correlation of event data, to all units in the theater, as required.
- Disseminating NETCOM-developed software distribution packages for all units in the theater.
- Managing the capabilities, availability, and performance of all theater units' systems.
- Coordinating distribution of system patches and notifying the NEC, enterprise operations center, TNCC, GCC, and all units in the theater of impending patches.
- Synchronizing the global address list for all units in the theater.
- Managing e-mail hubs to support all units in the theater.
- Providing theater-level technical support for problems escalated from the NEC.
- Overseeing operation, management, and security of the DODIN-A throughout the theater.
- Assessing mission impact of network events for the SC(T) commander.
- Operating and managing all Army-controlled items on the public or Defense Information Systems Agency side of the installation network infrastructure.
- Operating and managing selected systems and networks on the installation.
- Enforcing cybersecurity policies and reporting violations on Army networks.
- Identifying physical or logical property to address through the configuration management process.
- Providing guidance to Army NOSCs in theater through technical channels.
- Supervising Army use of DODIN operations tools in theater.
- Operationally managing communications assets provided by external organizations and agencies.
- Managing signal interfaces with joint and multinational forces, including host-nation support interfaces.
- Managing and controlling network transport and information services from the generating force to the operational force.
- Performing network management and enterprise systems management activities required to manage the information systems infrastructure and multi-organizational networks supporting the operational mission.
- Ensuring the cybersecurity tools are in place to for network protection and integrity, and to support secure access controls and connectivity.
- Performing change and release management to support units in the theater.
- Providing public key infrastructure support for Army users in theater.

2-59. The RCC coordinates with the ACOIC to oversee defensive cyberspace operations-internal defensive measures, network vulnerability assessment, and incident management within the theater. *Defensive cyberspace operations-internal defensive measures* are operations in which authorized defense actions occur within the defended portion of cyberspace (JP 3-12). In coordination with the ACOIC, the RCC—

- Coordinates threat-based vulnerability assessments with the supporting counterintelligence element.
- Conducts attack signature sensing and warning analysis.
- Develops mitigation strategies to support network defense and prevent data loss, including loss due to spillage. *Spillage* is a security incident that results in the transfer of classified information onto an information system not authorized to store or process that information (CNSSI 4009).
- Conducts the computer defense assistance program (penetration testing, network assistance visits, and network damage assessments) to support commanders and theater units.

INSTALLATION-LEVEL DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS INFRASTRUCTURE

2-60. Installation-level infrastructure delivers network services and automated information systems support at fixed locations. As the joint information environment matures, many of these functions (such as Defense Enterprise E-mail) will take place at the enterprise level.

2-61. The ***network enterprise center*** **is the facility that provides and acquires telecommunications and information management services on Army installations**. The NEC implements and manages enterprise services (including e-mail, user storage, office automation, collaboration, and cybersecurity) according to current policy, procedural guidance, and management procedures.

2-62. Centralized access to communications and DISN services at the NEC—

- Reduces congestion in the electromagnetic spectrum—each unit does not have to use separate transmission systems for network access.
- Reduces redundant efforts, since each unit does not have to maintain networking equipment and network administration. This still allows the flexibility of a unit performing its own network management and cybersecurity compliance activities using installation as a docking station.
- Improves cybersecurity posture by standardizing cybersecurity implementation across the installation with fewer potential points of failure.
- Reduces the cyberspace threat surface by maintaining fewer access points to the DODIN.

2-63. The NEC provides overall DODIN operations on its post, camp, or station, or within a designated geographic area. NECs plan and budget for network and information systems upgrades or replacements to meet customer requirements. NECs work with external organizations to ensure proper operation of installation-level components of DOD or Army-level networks and information systems. The NEC's DODIN operations responsibilities include—

- Providing customer access to the installation campus area network and information systems infrastructure.
- Providing service desk support and problem resolution for networks and information systems on the installation, or in the service area for which the NEC is directly responsible.
- Sharing information with other network managers about lessons learned and innovative ideas to support users.
- Implementing DODIN operations best business practices according to DOD, Army, NETCOM, and SC(T) policy and guidance.
- Coordinating with the strategic signal brigade to manage inter-installation networks and information systems affecting their supported organizations.
- Establishing and managing the cybersecurity program for the installation campus area network.
- Providing an installation as a docking station connection so units can connect their tactical systems to the installation campus area network.
- Managing network and information system resources in its area of operations under the direction of the supporting RCC, in coordination with the SC(T).
- Assessing mission impact of outages, network defense incidents, and other network issues for the RCC and strategic signal brigade.

- Responding to RCC direction to support problem resolution, change requests, and information assurance vulnerability management (IAVM).

2-64. The Army National Guard treats each state and territory as an installation (post, camp, or station). The state G-6 Directorate of Information Management provides NEC services to the units and members of that state or territory National Guard. Each state has an installation processing node and data center that hosts unique applications and data relevant to only that state or territory.

SECTION III – CORPS AND BELOW UNITS

2-65. Combat and combined arms units at echelons corps and below have adequate organic signal capabilities to conduct their standard missions without requiring outside signal support. The theater army may place additional signal assets, such as a theater tactical signal brigade, ESB, or other signal elements under OPCON of the corps or division, as required. For detailed information about available signal assets and requests for signal support, see FM 6-02. The RCC has overall responsibility for Army DODIN operations in the theater. All subordinate NOSCs take direction from the RCC and report status to the RCC through technical channels. The RCC maintains comprehensive situational understanding of the theater network.

CORPS AND DIVISION

2-66. The corps and division are headquarters organizations able to exercise command and control over land forces or serve as a joint task force headquarters. Both the corps and division have organic headquarters elements that command assigned or attached maneuver and support elements to meet mission objectives. Corps and division organic signal assets consist of the G-6 section and the signal portion of the signal, intelligence, and sustainment company. Having the signal support and DODIN operations capabilities organic to the headquarters enables unity of command and unity of effort. Commanders can readily leverage their portion of the network as a warfighting platform and align signal and network support to mission priorities. Figure 2-3 on page 2-16 shows the corps and below DODIN operations relationships and corresponding technical channels.

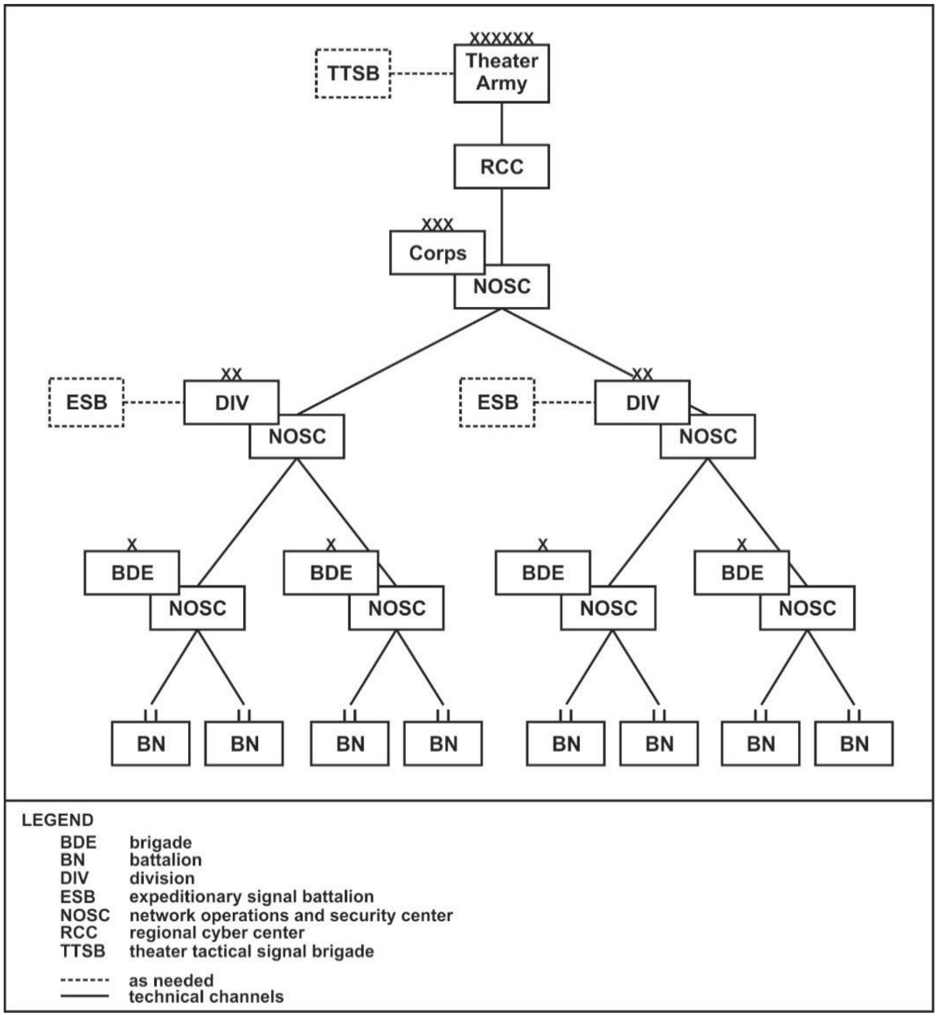


Figure 2-3. Department of Defense information network operations relationships-corps and below

Corps and Division G-6

2-67. G-6 sections in the corps and division are organized the same, except the grade structure. The G-6 controls DODIN operations within the unit's area of operations in compliance with joint, Army, and theater policies. The G-6 works closely with the higher headquarters G-6 or J-6, subordinate G-6, battalion or brigade signal staff officer (S-6), OPCON theater tactical signal brigade or ESB elements, and the organic signal, intelligence, and sustainment company to achieve integrated DODIN operations supporting the commander's intent. The G-6 staff plans and designs DODIN operations capabilities and support for command posts and subordinate units. The staff also provides training and readiness oversight for assigned and attached units.

2-68. The G-6 controls and monitors the network situational awareness view, including subordinate networks. The G-6 also helps integrate the network situational awareness view with that of the higher headquarters, for example the one controlled and maintained by a joint task force J-6. The situational awareness view consists of the status of all network components within the unit's area of operations, as well as the status of WAN links to theater, adjacent, and subordinate units.

2-69. Commanders have the authority to delay directed changes to their portion of the network. The commander may receive a network directive from higher headquarters that could adversely impact the unit's mission. In this case, issues will be resolved through command channels. Issue resolution requires close coordination between the commander, the G-6, and the higher headquarters commander and G-6 or J-6. The commander carefully considers the potential impact of delayed compliance with network directives and coordinates with higher headquarters and affected organizations to resolve compatibility issues and comply with the directed changes as soon as the tactical situation allows.

2-70. The G-6 section provides DODIN operations support to the main, tactical, and support area command posts and the mobile command group. G-6 DODIN operations activities integrate geographically separated units into the DODIN-A. Subordinate units' DODIN operations provide another level of management, which the G-6 coordinates as part of the overall DODIN operations plan.

2-71. Units without organic signal assets, such as functional support brigades, sometimes augment corps and divisions. The supported headquarters provides communications support for augmenting units, either with elements of their organic signal company or by requesting external, pooled assets through the request for forces process. For detailed information about available signal assets and requests for signal support, see FM 6-02. The G-6 integrates the supporting brigade and other signal assets into the network and provides DODIN operations for the supporting unit. The expanded DODIN operations mission may require augmenting the DODIN operations section with external capabilities from the supporting unit S-6 or from a theater tactical signal brigade or ESB.

2-72. The corps or division G-6 has these DODIN operations responsibilities—

- Recommending communications system and DODIN operations priorities for networks and systems to support the commander's priorities.
- Establishing procedures for relevant information and information systems to develop the common operational picture, in coordination with the assistant chief of staff, operations.
- Managing IT infrastructure to follow theater and Army-wide policies and standards, in coordination with the SC(T).
- Serving as the Army component G-6 in a joint task force, when designated. This mission may require equipment and personnel augmentation and support from the SC(T) and RCC.
- Serving as the joint task force J-6, if designated. This mission may require equipment and personnel augmentation.
- Advising the commander, staff, and subordinate commanders on communications networks and information services.
- Supervising DODIN operations in the area of operations.
- Monitoring, and making recommendations for, communications networks and information services.
- Preparing, maintaining, and updating communications systems operation estimates, plans, and orders. These orders often require configuration management changes across multiple organizations.
- Providing signal units with direction and guidance for plans and diagrams to establish the information network.
- Providing signal units with unit locations, organizational status, and communications requirements.
- Planning the integration of information systems.
- Developing, updating, and distributing signal operating instructions.
- Coordinating with signal elements of higher, adjacent, subordinate, and multinational units.
- Preparing and publishing communications system standard operating procedures for command posts.
- Coordinating, planning, and conducting spectrum management operations in the area of operations.
- Planning and coordinating with higher and lower headquarters for information system upgrades, replacement, elimination, and integration.
- Performing network vulnerability and risk assessments, in coordination with the assistant chief of staff, intelligence and the information operations officer, and according to Army and theater cybersecurity policies and procedures.

- Monitoring and disseminating information that changes warfighting function priorities and control measures.
- Coordinating, planning, and directing cybersecurity activities.
- Ensuring the command complies with Army and theater automation and systems administration policies, procedures, and standards.
- Validating user information requirements to support the mission.
- Establishing and disseminating the electronic battle rhythm, in coordination with the chief of staff, or assistant chief of staff, operations.
- Establishing policies and procedures for using and managing information tools and resources.
- Planning DODIN operations support for the corps or division command posts, and those of subordinate units.

Corps and Division G-6 Signal Operations

2-73. The corps and division G-6 signal operations sections consist of network management elements, cybersecurity and communications security (COMSEC) cells, plans elements, and signal systems support elements.

2-74. The network management element performs these DODIN operations functions—

- Manages the unit’s portion of the DODIN-A, from the applications through the connections to the theater network.
- Identifies, validates, establishes, plans, and manages communications requirements, including tracking the headquarters and subordinate units’ communications requirements within the area of operations.
- Installs, operates, maintains, and secures communications networks across the unit, including subordinate units, within the area of operations.
- Executes deliberate network modifications to meet the commander’s requirements.
- Installs, operates, and maintains COMSEC and transmission security devices to maintain confidentiality, integrity, availability, and authentication for transmission over private and public communications and media. For more information on COMSEC, see ATP 6-02.75. For more information on transmission security, see paragraph A-141.
- Performs fault, configuration, accounting, performance, and security management of network system components and services to ensure systems and applications meet the commander’s operational requirements.
- Manages the quality of service of the network services, including those provided by systems the G-6 does not directly control, for example, Global Broadcast System and combat service support very small aperture terminal.
- Conducts spectrum management operations, including frequency allocation and deconfliction with signal and non-signal emitters.
- Advises the commander, staff, and subordinate commanders on DODIN operations and network priorities to support the commander’s intent.
- Conducts information dissemination management and content staging so users can locate and retrieve voice and data information over SIPRNET, NIPRNET, and mission partner environment.
- Produces and distributes signal operating instructions.
- Prepares and publishes DODIN operations-related annexes and standard operating procedures.
- Prepares network reports for submission to the network management technician at G-6 and higher headquarters NOSCs.
- Provides network monitoring data to higher headquarters NOSCs and the network situational awareness view to local or subordinate users.
- Plans, integrates, and synchronizes network management with the cybersecurity, COMSEC, and information dissemination management cell.

2-75. The cybersecurity, COMSEC, and information dissemination management cell performs these DODIN operations functions:

- Manages cybersecurity compliance.
- Implements access controls for—
  - Information.
  - Information systems.
  - Networks.
- Manages software copies, updates, and security patches.
- Monitors for, detects, and analyzes anomalies that could cause network disruption, degradation, or denial.
- Executes response and restoration activities to resolve incidents that interrupt normal operations.
- Identifies threats against, and vulnerabilities of, the organization's information assets.
- Implements physical security from the outside perimeter to the inside operational space, including information system resources.
- Ensures the effectiveness of cybersecurity infrastructure (for example, firewalls and intrusion prevention system), and tools (Host Based Security System, antivirus, and software update service).
- Provides training and instruction on cybersecurity awareness, observations, insights, and lessons learned.
- Coordinates with higher and subordinate headquarters units to provide network defense-in-depth.
- Collaborates with the assistant chief of staff, intelligence to gain awareness of current threats and disseminate awareness of network anomalies.
- Conducts COMSEC management—
  - Plans and manages COMSEC operations, including subordinate units.
  - Implements procedures for detecting and reporting COMSEC insecurities.
  - Receives, transfers, accounts for, safeguards, and destroys COMSEC material.
  - Ensures users employ COMSEC key only for its intended purpose within the network.
- Conducts information dissemination management and content staging.
- Implements, manages, and maintains user services (web services, e-mail, database, collaboration tools, and mass storage).
- Plans and coordinates procedures for contingency operations, including continuity of operations and data recovery.
- Provides collaboration, messaging, and storage services to support information advantage.
- Prioritizes information resources.
- Monitors information delivery status and integrates it into the network situational awareness view.
- Manages information system and network support activities.
- Disseminates the common operational picture and executive information.

2-76. The plans element performs these DODIN operations functions:

- Prepares, maintains, and updates command information management estimates, plans and orders, including—
  - Mission analysis products.
  - Annex H (signal) to corps or division plans and orders.
  - Telecommunications plan.
  - Network management plan.
  - Information management plan.
- Establishes procedures to employ relevant information and information systems to develop the common operational picture, in coordination with the assistant chief of staff, operations.
- Coordinates local network capabilities and services.

- Conducts spectrum management operations.
- Plans combat visual information documentation.
- Coordinates future network connectivity, information dissemination management, and network interface with joint and multinational forces, including those of the host nation.
- Coordinates, plans, and directs development of the network situational awareness view for the main command post.
- Plans the transition of responsibility for the tactical network from the corps or division to permanent theater signal assets.

2-77. The signal systems support element performs these DODIN operations functions:

- Installs, operates, maintains, and secures servers for SIPRNET, NIPRNET, and mission partner environment to support the main, tactical, and support area command posts.
- Manages installation and operation of main, tactical, and support area command post local area networks, including cable and wire installation and troubleshooting.
- Establishes and operates the corps or division service desk to provide user assistance for voice, video teleconferencing, and e-mail services.

CORPS AND DIVISION NETWORK OPERATIONS AND SECURITY CENTERS

2-78. The NOSC performs the DODIN operations activities required to operate and secure the network within the corps or division area of operations. The NOSC responds to shifting network priorities to support the tactical plan and extend the DODIN's strategic capabilities to tactical formations. Signal elements coordinate with the NOSC to install, operate, maintain, and secure the network.

2-79. The NOSC establishes the network and provides operational and technical support to all signal elements in the area of operations. It also provides network status and running estimates to operations planners to support tactical operations.

BRIGADE COMBAT TEAM AND MULTIFUNCTIONAL SUPPORT BRIGADE

2-80. The BCT has organic signal assets that provide network transport and information services to support the commander's information requirements. The BCT's signal elements provide 24-hour communications networks to its formations, and install, operate, maintain, and secure these systems.

2-81. Each multifunctional support brigade (maneuver enhancement, field artillery, combat aviation, sustainment, or security force assistance) has an organic signal company. This company provides the brigade's tactical communications support.

BRIGADE COMBAT TEAM AND MULTIFUNCTIONAL SUPPORT BRIGADE S-6 RESPONSIBILITIES

2-82. The brigade S-6 maintains DODIN operations in the brigade area of operations in compliance with joint, Army, and theater policies. The brigade S-6 may also serve as the Army component S-6 in a joint task force. The brigade S-6 works closely with its higher headquarters G-6 or J-6 and the brigade signal company to integrate DODIN operations while meeting the commander's intent. The brigade S-6 controls and monitors the status of the brigade portion of the DODIN-A, including subordinate units, to maintain network situational understanding. The S-6 also helps integrate the brigade network situational awareness view with that of the higher headquarters, such as corps or division G-6 or joint task force J-6.

2-83. The brigade commander has the authority to delay directed changes to the brigade portion of the network. The brigade commander may receive a network directive from higher headquarters that could adversely impact the brigade's mission. In this case, issues are resolved using command channels. Resolving issues requires close coordination between the brigade commander, the brigade S-6, and the higher headquarters commander and G-6 or J-6. To resolve compatibility issues and comply with the directed changes, the commander carefully considers the potential impact of delayed compliance with network directives and coordinates with higher headquarters and affected organizations as soon as the tactical situation allows.

2-84. If units without organic signal assets augment the brigade, or if the brigade must establish a network beyond its organic capabilities, the brigade S-6 defines communications and network support requirements, based on the situation and mission. The operational chain of command validates requests for signal support they cannot source internally and forwards them to United States Army Forces Command for approval and resourcing. The brigade S-6 assumes DODIN operations responsibility for the augmenting elements. See FM 6-02 for detailed information about available signal assets and requests for signal support.

2-85. The brigade S-6 staff plans DODIN operations capabilities and network support for brigade command posts and subordinate units. The S-6 section personnel are part of the brigade command post staffing to support the commander's critical information requirements. Figure 2-4 depicts the brigade DODIN operations relationships and technical channels with higher and lower headquarters.

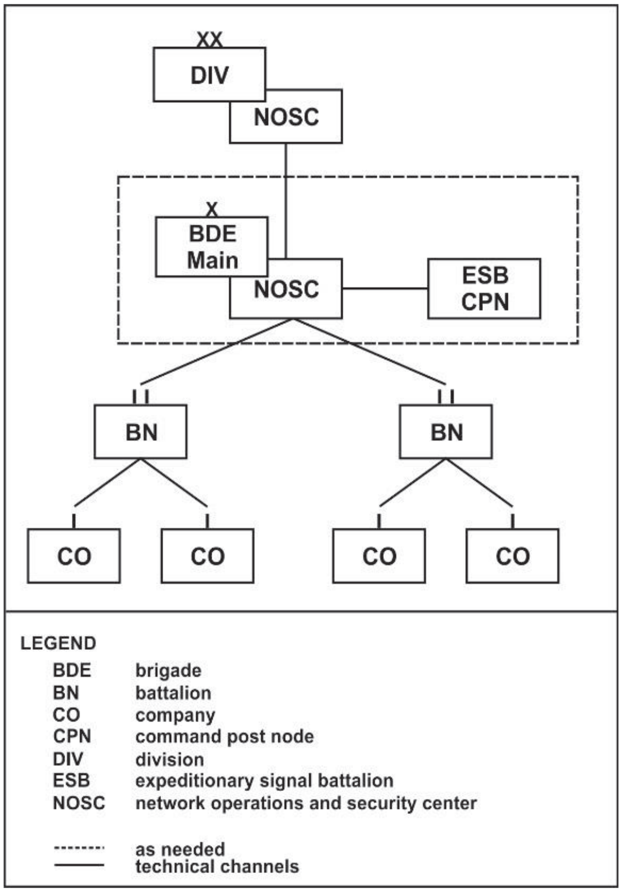


Figure 2-4. Brigade Department of Defense information network operations relationships

Brigade Combat Team and Multifunctional Support Brigade Network Operations and Security Center

2-86. The brigade NOSC is the brigade's network control center that plans and directs DODIN operations. Designated personnel from the S-6 section staff the brigade NOSC with the same responsibilities as higher-level NOSCs, scaled to the size of the unit and operation.

2-87. The brigade NOSC reports directly to the brigade S-6. The NOSC uses the brigade's organic WIN-T network management capability to configure, monitor, and manage the brigade WAN. The brigade NOSC supports the S-6 section in installing, operating, maintaining, and securing the command post local area networks, and prioritizes information dissemination across the WAN. Under the direction of the brigade S-6, the NOSC—

- Conducts brigade spectrum management operations.
- Plans and manages the brigade information network.
- Plans and manages cybersecurity, including—
  - Firewalls.
  - Intrusion detection systems.
  - Access control lists.
  - Key management and distribution.
  - Cybersecurity compliance.
- Plans and manages information dissemination management and content staging for the brigade—user profiles, file and user priorities, and dissemination policies—in coordination with higher headquarters NOSCs and the supporting RCC.
- Evaluates the brigade's network and communications relay requirements.
- Conducts DODIN operations to support the unit's mission.
- Advises operation planners of current network status, and provides estimates to support tactical operations.

Network Management Cell

2-88. The network management cell operates, maintains, and sustains networked systems to provide the desired level of quality and guarantee availability. The network management cell—

- Manages the brigade network, from the applications on brigade platforms through the connections to the division network.
- Identifies, validates, and manages communications requirements, including the headquarters and subordinate units' requirements within the area of operations.
- Monitors network performance and quality of service, including interoperability of the brigade network with external networks.
- Installs, operates, and maintains communications networks, including subordinate units within the area of operations.
- Executes deliberate network modifications to meet the commander's requirements.
- Manages quality of service for brigade network services, including those systems not directly controlled by the S-6, for example, Global Broadcast System and combat service support very small aperture terminal.
- Installs and maintains COMSEC and transmission security devices for secure transmission over private and public communications networks and media.
- Performs fault, configuration, accounting, performance, and security management of network system components and services (situational understanding, voice, video, data, and imagery) to ensure systems and software applications meet the commander's operational requirements.
- Conducts spectrum management operations.
- Advises the commander, staff, and subordinate commanders on DODIN operations and network priorities to support the commander's intent.
- Prepares and publishes DODIN operations related annexes and standard operating procedures.
- Develops, produces, updates, and distributes signal operating instructions.
- Plans, coordinates, integrates, and synchronizes network management with the cybersecurity and COMSEC cell and the signal system integration and oversight and information dissemination management cell.
- Reports network status to the network management technician, brigade S-6, and division NOSC.
- Provides the network situational awareness view to the division NOSC and authorized recipients in the brigade.

Cybersecurity and Communications Security Cell

2-89. The cybersecurity and COMSEC cell monitors and manages activities to provide data confidentiality, integrity, availability, and protection against unauthorized access. The brigade S-6 cybersecurity and COMSEC cell—

- Implements access controls for—
  - Information.
  - Information systems.
  - Communications networks.
- Manages software copies, updates, and security patches.
- Executes response and restoration activities to resolve incidents that interrupt normal operations.
- Conducts risk assessments to identify threats against, and vulnerabilities of, the organization's network.
- Manages cybersecurity compliance.
- Implements physical security, from the outside perimeter to the inside operational space, including all information system resources.
- Ensures the effectiveness of cybersecurity infrastructure, using firewalls and intrusion prevention system and tools, for example, host-based prevention, antivirus, and software update service.
- Monitors for, detects, and analyzes anomalies that may disrupt, degrade, or deny network service.
- Plans and manages brigade COMSEC operations, including subordinate units, and implements COMSEC incident detection and reporting procedures.
- Receives, transfers, accounts for, safeguards, and destroys COMSEC material.
- Ensures users employ COMSEC key only for its intended purpose on the network.
- Provides cybersecurity awareness, observations, insights, and lessons learned training.
- Coordinates with higher headquarters, and directs subordinates, to provide network defense-in-depth.
- Collaborates with the intelligence staff officer to gain threat awareness and disseminate awareness of network anomalies.
- Plans, coordinates, integrates, and synchronizes cybersecurity activities with the network management cell and the signal systems integration and oversight and information dissemination management cell.

Signal Systems Integration and Oversight and Information Dissemination Management Cell

2-90. The signal systems integration and oversight and information dissemination management cell provides training and maintenance oversight for the brigade signal company. It monitors and manages information storage and dissemination. The brigade S-6 signal systems integration and oversight and information dissemination management cell—

- Plans and manages the tactical radio network.
- Installs, operates, and maintains automated information systems.
- Enables the discovery of information, services, and applications.
- Provides collaboration, messaging, and information storage to support information advantage.
- Prioritizes information resources.
- Monitors information delivery status and integrates with overall situational understanding.
- Supports IT life cycle management.
- Integrates systems across the unit and with Army and joint, inter-organizational, and multinational elements.
- Helps install user information systems.
- Implements the tactical intranet at brigade and below.
- Provides system administration and local area network management.
- Performs service desk functions and problem tracking.

- Plans, coordinates, integrates, and synchronizes signal systems integration and oversight and information dissemination management with the network management cell and the cybersecurity and COMSEC cell.

MANEUVER AND SUPPORT BATTALIONS AND COMPANIES

2-91. Maneuver battalions and companies receive tactical internet support using organic WIN-T assets, managed by the brigade NOSC. Support battalions and companies receive their tactical internet support from elements of the brigade signal company, which also provide DODIN operations for the supported unit. Tactical battalion and below units have no inherent DODIN operations roles in the upper tier tactical internet. See ATP 6-02.60 for more information about WIN-T, and ATP 6-02.53 for information on DODIN operations in the lower tier tactical internet.

FUNCTIONAL SUPPORT BRIGADES

2-92. Theater-level commands may receive specialized support from functional support brigades. Examples of functional support brigades include—

- Military police.
- Engineer.
- Air and missile defense.
- Medical.
- Chemical, biological, radiological, and nuclear.
- Civil affairs.

2-93. Functional support brigades may be attached or OPCON to a corps or division. These brigades do not have organic signal companies or assets. They receive their signal support from pooled assets, such as an ESB, or from the internal assets of the supported unit. The supported unit assumes DODIN operations responsibility for supporting units' requirements. This expanded DODIN operations role may require DODIN operations augmentation to manage the network. For more information on signal support for functional brigades, see Army doctrine for signal support.

Chapter 3

Department of Defense Information Network Operations Activities

This chapter provides the framework for executing DODIN operations at all levels. It describes and discusses DODIN operations activities; defines and describes DODIN operations functional activities; identifies the echelons and organizations that support the activities; and provides details on how organizations support each specific DODIN operations activity. This support information includes inter-organizational relationships associated with specific DODIN operations activities. This chapter identifies joint implications related to DODIN operations execution and support.

DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS SUPPORT TO OPERATIONS

3-1. Tactical DODIN operations support commanders conducting joint and Army operations. DODIN operations capabilities—

- Establish and maintain information connectivity and common services infrastructure between applications—sensors, handheld devices, computers, vehicles, command posts, data centers, and sanctuary locations.
- Manage efficient movement and storage of critical information, according to the commander's priorities and operational imperatives.
- Protect applications, information devices, and information, whether in transit or at rest.

3-2. Effective DODIN operations enable a robust network and protect information from unauthorized access and exploitation. DODIN operations allow the commander to tailor the network to the situation and phase of operation. Tailoring the network allows the commander to maintain informed situational understanding and provides the ability to control and react to the changing operational environment. Measures to tailor the network include reallocating bandwidth, establishing or terminating links, or performing procedures to operate with network degradation.

3-3. DODIN operations support the commander and staff in all operational phases by—

- Rapidly initializing information systems and networks for operations and security.
- Enabling access to information from multiple locations, as the situation dictates.
- Allowing the commander to monitor network status and balance network demands.
- Providing the means to recover from network outages without requiring full re-initialization or data reload.
- Providing flexible reconfiguration and scaling of network resources and user services. Reconfiguration and scaling includes bandwidth allocation tailoring essential services to the commander's priorities, allowing them to continue uninterrupted in a degraded environment.
- Enabling formulation of continuous running estimates.
- Enabling information sharing with lower, higher, and adjacent organizations to gain early threat understanding.
- Facilitating dissemination of tactical orders, appropriate graphics, and overlays to subordinate units.

DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS TENETS

3-4. DODIN operations tenets are the principles and doctrinal underpinning of the DODIN operations framework. These tenets encompass the DODIN operations framework, authority, and operational relationships—

- **Define DODIN operations authority**—specify who is responsible for what portion of the network within the assigned area of operations.
- **DODIN operations aligned with the operational chain of command**—the commander's designated DODIN operations element executes retained authorities.
- **DODIN operations executed based on DODIN operations element capability**—delegate authorities to subordinate commanders, as required, based on their capabilities.
- **Assigned DODIN operations element responsible for the full scope of cybersecurity**—the element is responsible for the cybersecurity posture of the network across the full scope of their designated DODIN operations authority.

DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS EVENTS

3-5. A DODIN operations event is any occurrence that can adversely affect the operational readiness of the DODIN. The scope of an event's effects and the DODIN operations structure determine the event category. The event category determines the supported and supporting relationships between commands and DODIN operations facilities for event response. Commanders base their DODIN operations response on the nature of the event and the current situation. There are three categories of DODIN operations event—

- **Global DODIN operations events** can affect the worldwide operational readiness of the DODIN and require a coordinated response. Commander, Joint Force Headquarters-DODIN issues orders and directions for global DODIN operations event response through the USCYBERCOM Joint Operations Center.
- **Theater DODIN operations events** can affect DODIN operations across a theater of operations. The GCC is the supported commander for theater DODIN operations events, with USCYBERCOM as a supporting command.
- **Non-global DODIN operations events** affect functional combatant commands or other entities that are neither global nor theater-specific. Commander, USCYBERCOM is the supported commander for non-global DODIN operations events.

POLICIES, STANDARDS, PLANNING, AND DESIGN

3-6. DODIN operations policies and standards provide a common foundation and general guidance for provisioning and managing DODIN operations capabilities. DODIN operations capabilities require planning and design to be effective, regardless of the affected organization, system, or technology. Capability planning and design are especially important for the tactical environment, because of the potential for limited connectivity and the fog of war.

GLOBAL POLICIES AND STANDARDS

3-7. Global DODIN operations policies and standards are approved and issued from the global DOD and Army levels, and apply to DODIN operations capabilities at all levels. These policies and standards define general system configurations, procedures, protocols, and information exchange requirements. Global policies and standards enable compatibility between elements and reduce the disruption caused by task organization. Adherence to global policies and standards is critical to ensure compatibility between tactical units and strategic service providers, and between units that come together from different geographic areas and commands.

3-8. Tactical units sometimes need support from non-tactical units due to physical and manning limitations. DODIN operations capabilities must be uniform and well-defined for effective strategic support. Global policies standardize DODIN operations capabilities without impairing tactical commanders' ability to manage and allocate their network assets.

3-9. Some examples of global DODIN operations policies and standards include—

- Protocols and port configuration guidelines.
- Inter-organizational information exchange requirements.
- Change approval and change implementation responsibilities.
- Reportable configuration management information.

Global Policies and Standards—Echelons and Organizations

3-10. The Department of the Army Chief Information Officer/G-6 establishes global DODIN operations policies and standards for the Army. The Chief Information Officer/G-6 staff continually reviews, and periodically updates, global policies and standards based on recommendations from tactical organizations, enterprise architecture requirements, and relevant technological advancements.

Global Policies and Standards—Joint Implications

3-11. Global Army DODIN operations policies incorporate global joint policies. Army DODIN operations policymakers also staff policies that arise in the tactical community through joint channels to prevent policy conflicts when Army tactical elements operate in a joint environment.

Temporary Exceptions to Policies and Standards

3-12. Isolated changes or additions to DODIN operations policies and standards threaten enterprise-wide compatibility and efficiency. Tactical DODIN operations policies and standards cannot always adhere to the drawn-out policy change process that exists in the fixed-station environment, because tactical operations are time-sensitive and volatile. Mission-specific factors may require temporary policy changes, but commanders should minimize exceptions to DODIN operations policy to preserve compatibility.

> ***Note.*** Temporary changes to network policies may be more stringent or strict than the global policies (for example, blocking a port or protocol), but they may not be less stringent or strict.

3-13. The operational chain of command approves additions, changes, or exceptions to tactical DODIN operations policy. The next higher echelon must grant prior approval if an echelon wishes to add to, change, or bypass a tactical DODIN operations policy. For example, if a brigade commander wants to issue a policy blocking a particular network protocol, prior approval from higher headquarters is required. Prior coordination makes it less likely the policy change will inadvertently impair the functionality of the unit's assets, or adversely affect the broader DODIN operations state. If a policy addition or change is likely to damage overall network health or compatibility, the approving headquarters will carefully consider whether the advantage gained by the policy change outweighs the potential impact.

3-14. In some cases, a policy change or addition requires approval from an echelon above the requesting organization's parent headquarters. This requirement would occur when a proposed policy change may affect network-wide security or functionality. In this case, the parent headquarters forwards the request to the echelon with approval authority. In general, echelons above the organization's parent headquarters only require notification of DODIN operations policy modifications.

3-15. Policy exceptions route through the operational chain of command, which compiles and reviews this data to recommend changes and additions to global DODIN operations policies and standards.

3-16. In tactical scenarios, urgent situations may arise where there is no time for the formal approval process before issuing policy guidance. The unit commander, advised by the signal staff, makes risk decisions and takes responsibility for network impact. In these cases, the commander must inform higher and affected organizations as soon as the tactical situation allows.

Temporary Exceptions to Policies And Standards—Echelons and Organizations

3-17. For the BCT or functional support brigade and below, the brigade S-6 defines and maintains temporary exceptions to policies and standards. These short-term exceptions are based on mission requirements and refined from global policies and standards and any mission-specific policies and standards implemented by the operational chain of command. The brigade provides policy and standards guidance to subordinate organizations within its area of operations.

3-18. The corps and division G-6 define and maintain temporary exceptions to policies and standards to support the corps and division. These exceptions are based on the corps or division mission requirements, and further refined from global policies and standards, as well as any mission-specific policies and standards implemented by higher headquarters. The corps and division provide policy and standards guidance for units in their area of operations, including BCTs, support brigades, and ESBs. The corps and division also consider how changes may affect adjacent and supporting organizations.

3-19. The theater army G-6 defines and maintains temporary DODIN operations policy and standard exceptions within the theater. The G-6 bases these exceptions on the ARFOR mission requirements, global standards, and theater joint policies and standards. The theater army provides policy and standards guidance to its assigned or attached corps and divisions, directly reporting brigades, and other theater assets. The theater army considers how changes might affect compatibility with other organizations and Services in the theater, with policy guidance and direction from the TNCC.

Temporary Exceptions to Policies and Standards—Joint Implications

3-20. The joint chain of command creates joint organizational and mission-specific policies and standards. Army tactical formations incorporate both joint and Army tactical DODIN operations policies and standards. The signal staff notifies their Army and joint parent headquarters if Army and joint guidance conflict. The chain of command clarifies and reconciles conflicting guidance.

DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS PLANNING

3-21. Because they are complex and have wide-ranging impact, DODIN operations require deliberate staff planning and coordinated execution through the military decision making and operations processes to ensure the network supports the mission and commander's intent, the same as any weapons system. Signal staffs formulate DODIN operations plans through the military decision-making process. NOSCs implement those plans and control the network through technical channels. Commanders exercise command authority over their portions of the network.

3-22. DODIN operations planning involves collecting, validating, and prioritizing user requirements. Planners align these requirements with the mission and commander's intent, allocate technical and organizational resources, and prepare the signal annex to orders.

3-23. DODIN operations plans describe how DODIN operations support the commander's intent and the concept of operations through actions taken to gain and maintain access to cyberspace. These actions include allocating resources; maintaining configurations; continuously monitoring performance and effectiveness; responding to network events; and performing security functions to install, operate, maintain, and secure the NIPRNET, SIPRNET, and the Joint Worldwide Intelligence Communications System. The DODIN operations appendix to the operation order includes—

- Network node types and locations.
- Primary, alternate, contingency, and emergency communications plans.
- Signal integration with intelligence and electronic warfare to support network situational understanding.
- Friendly forces, capabilities, and mission in the operational area.
- Enemy force locations, capabilities, and expected courses of action.
- Joint, inter-organizational, and multinational integration and data exchange.
- Mission priorities for signal support.

> ***Note.*** When establishing a primary, alternate, contingency, and emergency plan, ensure alternate or contingency methods of communications do not rely on the primary method. For example, Voice over Internet Protocol is a poor alternate if the primary means is network data, because when the primary is down the alternate may also be down.

3-24. DODIN operations planners consider current intelligence estimates and adversary capabilities when formulating their plans. Planning includes contingencies for how the network will continue to operate in the contested information environment.

> ***Note.*** See FM 6-02 for more information on preparing the signal annex to operation orders.

Department of Defense Information Network Operations Planning—Echelons and Organizations

3-25. All organizations in the operational chain of command take part in DODIN operations planning. As each echelon develops its plans, commanders provide guidance to subordinates. The lower echelon uses this guidance to create or refine their DODIN operations plans. Mission planning is a continual process. For detailed information on mission planning, refer to ADP 5-0 and FM 6-0.

3-26. Theater-level DODIN operations planning for Army starts with the theater army G-6. The theater army G-6 develops theater network requirements and manages the activities and resources needed to install, operate, maintain, and secure operational and strategic networks supporting Army forces in the theater. The theater army G-6 ensures proper integration and protection of tactical networks employed by maneuver units and the operational Army at the corps, division, and brigade levels to ensure tactical commanders have the quality of service they need to enable mission success.

3-27. The theater army G-6 formulates DODIN operations plans for the theater army; provides planning guidance to assigned or attached corps and divisions, directly reporting BCTs, and support brigades; coordinates planning between subordinate organizations; and coordinates with the SC(T) throughout the planning process.

3-28. DODIN operations planning may include coordination between theaters. The theater army performs inter-theater coordination to support deploying or redeploying organizations.

3-29. The corps and division G-6 formulate their DODIN operations plans to support the corps and division; provide planning guidance to BCTs and support brigades; and coordinate planning between subordinate BCTs and support brigades.

3-30. At the brigade and below, the brigade S-6 formulates DODIN operations plans. The brigade provides DODIN operations planning support to subordinate maneuver battalions.

Department of Defense Information Network Operations Planning—Joint Implications

3-31. Both the joint and Army chains of command plan DODIN operations. Army tactical organizations incorporate DODIN operations planning guidance from their higher joint headquarters. The signal staff notifies their Army and joint parent headquarters if Army and joint DODIN operations planning guidance conflict. The chain of command clarifies and reconciles conflicting guidance.

CAPABILITY EMPLOYMENT CONFIGURATION

3-32. Guidance from operation orders and annexes usually dictates the configuration for a DODIN operations capability to support a specific mission. DODIN operations capability employment configuration supports and provides feedback for DODIN operations planning. DODIN operations capability employment configuration includes—

- Developing operational configurations to provide required IT support capabilities.

- Developing configurations for communications network, system, and security capabilities to support tactical DODIN operations.
- Developing operational configurations for internetworking of DODIN operations applications, systems, networks, and communications infrastructure.

CAPABILITY EMPLOYMENT CONFIGURATION—ECHELONS AND ORGANIZATIONS

3-33. All organizations in the operational chain of command take part in configuring DODIN operations capabilities, either directly or in a coordinating or supporting role. As each echelon configures their DODIN operations capabilities, they provide information to subordinate echelons. The highest echelon integrating a system across multiple subordinate units initiates the employment configuration process. This process extends down to the echelon that operationally manages the affected system. Signal staffs at lower echelons use this guidance to configure their DODIN operations capabilities.

3-34. The RCC configures theater-wide DODIN operations capabilities—those capabilities resident at, or under direct control of the RCC. The theater army G-6 configures DODIN operations capabilities within the theater army headquarters; provides configuration guidance to corps, divisions, and directly reporting BCTs; coordinates capability employment configuration between subordinate organizations; and coordinates with the SC(T) in the configuration process. The theater army focuses its capability employment configuration on DODIN operations interoperability across the theater.

3-35. Capability employment configuration requires coordination between theaters, especially during force buildup, deployment, and redeployment. The theater army performs inter-theater coordination to support deploying and redeploying units.

3-36. The corps and division G-6 configure DODIN operations capabilities for the corps and division, respectively; provide configuration guidance for their subordinate units, including BCTs, support brigades, and attached ESBs; and coordinate capability configuration between subordinate BCTs and support brigades. The corps and division focus their capability employment configuration on facilitating DODIN operations interoperability between echelons.

3-37. The brigade S-6 configures DODIN operations capabilities for the brigade and subordinate maneuver battalions in the upper tier tactical internet. See ATP 6-02.53 for more information about DODIN operations in the lower tier tactical internet.

CAPABILITY EMPLOYMENT CONFIGURATION—JOINT IMPLICATIONS

3-38. The ARFOR G-6 configures DODIN operations capabilities for the ARFOR headquarters; provides configuration guidance for its area of operations, including corps, divisions, BCTs, support brigades, and attached ESBs; and coordinates capability configuration between subordinates within its area of operations. The ARFOR focuses its capability employment configuration on facilitating joint DODIN operations interoperability, and provisioning services to meet mission requirements.

3-39. The Army and joint chains of command configure their tactical DODIN operations capabilities and help configure DODIN operations capabilities to support assigned Army organizations. Army organizations incorporate joint configuration guidance. The signal staff notifies their Army and joint parent headquarters if Army and joint guidance conflict. The chain of command clarifies and reconciles conflicting guidance.

TACTICAL DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS

3-40. Tactical DODIN operations are the activities to manage, support, execute, and evaluate a stable tactical communications infrastructure. These activities use Army and industry best practices to assure access to reliable network services across all phases of operations.

Tactical Department of Defense Information Network Operations Reporting

3-41. Theater army, corps, division, and brigade organizations maintain situational understanding of Army networks and systems within their areas of operations for the senior commander. DODIN operations reports identify critical network outages and the confidentiality, integrity, and availability of Army networks. Tactical reporting may also provide the first indication of a cyberspace or electronic warfare attack. NOSCs report status and provide situational awareness to their next higher echelon NOSC through technical channels. The highest echelon network operations and security center in the deployed network enclave reports to the RCC. The RCC reports theater DODIN operations actions and status to the ACOIC.

Tactical Department of Defense Information Network Operations Reporting—Joint Implications

3-42. When the theater army is not acting as the joint task force headquarters, it reports DODIN operations status to its joint task force J-6. The joint community identifies DODIN operations reporting responsibilities to a joint command and the theater army.

SHARED SITUATIONAL UNDERSTANDING

3-43. DODI 8410.02 mandates shared network situational understanding. DODIN operations situational understanding involves collecting status data from various sources to provide the relevant situational awareness view for a specific user or set of users. Each organization can customize the situational awareness view to meet its specific requirements. The common source of theater DODIN operations status information allows users to filter the display to only the data they need. Comprehensive network situational understanding, combined with current intelligence estimates, allows the cyberspace electromagnetic activities section to synchronize signal capabilities with cyberspace and electronic warfare operations.

Shared Situational Understanding—Echelons and Organizations

3-44. The BCT NOSC ensures systems in its area of operations are equipped and configured to report DODIN operations status data to higher echelons.

3-45. The corps and division NOSCs ensure DODIN operations systems in their areas of operations are equipped and configured to report required status data to higher-level Army and joint DODIN operations authorities. The RCC maintains the consolidated network status for Army forces in theater and reports to the ACOIC.

Shared Situational Understanding—Joint Implications

3-46. Effective DODIN operations require that each successive level of DODIN operations management maintain awareness and understanding of the network. Army DODIN operations organizations provide situational awareness data to their higher-level joint DODIN operations organizations in their respective theaters.

CHANGE MANAGEMENT

3-47. Change management is a deliberate process to identify, document, approve, and implement variances from baseline configurations. The goal of change management is to ensure standardized methods for network modifications. Standardization helps facilitate changes while reducing their negative effects.

3-48. The unit’s signal staff performs change management for user systems and DODIN operations capabilities. The supporting signal unit (for example the corps, division, or brigade signal company) performs change management for the network and network capabilities. Change requests are formal proposals in response to incidents or problems, requests for temporary policy exceptions, or support for emerging mission requirements. Any unit or signal staff within the operational chain of command, up to and including the theater army, may start the change management process by submitting a request for change.

3-49. On submission, a request for change routes through the operational chain of command to the approval authority. In routing, the request for change passes through each intermediate command echelon. Advance coordination ensures the chain of command is aware of all requests and facilitates orderly implementation of approved changes. Plans and engineering personnel at each echelon examine the request to ensure it is workable, justified, and does not violate network, system, or security policies.

3-50. Change approval authority corresponds to operational management responsibilities. If an echelon operationally manages a particular system, it can also approve changes to that system, as long as the proposed changes do not violate standing policy or guidance. If the change would violate policy or guidance, the echelon requiring the change may request a temporary policy exception (refer to the temporary exceptions to DODIN operations policies and standards section at paragraph 3-12).

3-51. The unit commander usually delegates approval authority for network change requests to the signal staff. The signal staff principal may retain and execute this authority, or further delegate it to DODIN operations personnel in the unit.

3-52. When the designated approving authority approves a change, the validated request passes to the echelon(s) that implements the change. All affected organizations coordinate the change before execution. Advance coordination prevents failure or compromise of services in their area of operations.

3-53. High-level echelons, such as the GCC, may also initiate changes. For example, a system may need an urgent patch to mitigate a newly identified vulnerability. Urgent change requests may bypass the formal approval process, but still require coordination with the ARFOR and affected tactical units to determine when and how to implement the change. If the ARFOR decides a change originating from the GCC carries an unacceptable risk of disrupting user services, it may request delay or deferral through its chain of command. This type of change request is rare.

3-54. The echelon that operationally manages a system always implements changes for that system. In the tactical networking environment, situations commonly arise that require immediate action. In such emergencies, personnel may need to implement changes outside their usual scope of responsibility.

3-55. Changes made to user systems, DODIN operations capabilities, and networking capabilities often involve configuration changes. These changes include software updates, configuration modifications, and hardware replacement. Personnel making network changes record them in an automated configuration management system. The configuration management system notifies affected organizations of any configuration modifications resulting from change requests. All BCT and above units can access this system. Army organizations, such as the theater army and the ACOIC, also receive configuration change notifications to maintain situational understanding across the enterprise.

> ***Note.*** Change management and configuration management are separate, but interdependent activities. Specifically, configuration management documents change management actions.

Change Management—Echelons and Organizations

3-56. The brigade S-6 performs change management for assets within the brigade's area of operations, supported by the brigade signal company and assigned or attached signal personnel. At the brigade and below, the S-6 may approve or deny change requests. If they do not have approval authority, they escalate them to the next higher headquarters for processing. Brigade DODIN operations personnel implement changes on all systems they operationally manage.

3-57. The corps and division G-6 perform change management for assets within their area of operations, supported by the corps and division signal, intelligence, and sustainment companies and assigned or attached signal personnel. The G-6 may approve or deny change requests, or escalate them to the next higher headquarters for further processing. Corps and division DODIN operations personnel implement changes on all systems they operationally manage.

3-58. The ESB performs designated change management functions for their supported unit. It initiates and processes change requests related to the DODIN operations capabilities it provides. The ESB may also exercise approval authority for change requests from the supported signal staff, if so delegated.

3-59. The theater army performs change management functions for RCC support services. The theater army is the approval authority for change requests for Army networks in the theater. The theater army coordinates these changes with all affected organizations, as defined in the change implementation process.

CHANGE MANAGEMENT—JOINT IMPLICATIONS

3-60. Joint guidance governs change management within joint organizations or between Army and joint organizations. Army personnel supporting these functions operate within joint guidance while also adhering to Army change management procedures as much as the joint (higher level) guidance allows.

3-61. The theater army G-6, supporting ESBs, and assigned or attached signal personnel perform change management for assets within their areas of operations. The theater army G-6 may approve or deny change requests, or escalate them to the joint headquarters J-6 for further processing. The joint task force exercises change approval authority for all jointly managed systems that need approval above the corps and division levels. The theater army G-6 implements changes on all systems it operationally manages. The ARFOR and joint task force also take part in change notification and approval for all DODIN operations assets within the joint operations area.

CONFIGURATION MANAGEMENT

3-62. *Configuration management* is a discipline applying technical and administrative direction and surveillance to: (1) identify and document the functional and physical characteristics of a configuration item; (2) control changes to those characteristics; and (3) record and report changes to processing and implementation status (JP 6-0). DODIN operations configuration management supports identifying, controlling, maintaining, and verifying systems and devices associated with DODIN operations capabilities. Configuration item information includes hardware, software, device configuration, and version information. Activities associated with configuration management include—

- Identifying all configuration items.
- Controlling configuration items.
- Maintaining current and historical configuration item status.
- Verifying configuration item status.

3-63. The acquisition and life cycle management process includes determining what to track as a configuration item, what information to collect, and what information to store for each configuration item. Program managers establish and control product attributes and technical baselines for new equipment and systems across the total system life cycle. Policy dictates how often to update information for each configuration item, based on mission factors including operational tempo and bandwidth constraints.

3-64. The unit's signal staff performs configuration management for their user systems and DODIN operations capabilities. The supporting signal unit, such as a signal company or ESB, performs configuration management for the network and network capabilities.

3-65. The Defense Information Systems Agency's security technical implementation guides provide DOD-wide configuration standards for cybersecurity and cybersecurity-enabled devices and systems. The security technical implementation guide requirements are available from the Information Assurance Support Environment Website (requires DOD-approved certificate login).

CONFIGURATION MANAGEMENT—ECHELONS AND ORGANIZATIONS

3-66. Each echelon ensures subordinates in its area of operations perform the necessary configuration management activities and report them in the configuration management database. Designated network management personnel at each echelon share read-only access of all network resources to facilitate this process.

3-67. The RCC maintains an authoritative, distributed configuration management database for the theater that supports the Army global configuration management database. The RCC compiles this database using input from all DODIN operations organizations in the theater.

3-68. Brigade S-6 personnel manage configurations for the brigade and below, assisted by the organic signal company, supporting ESBs, and other supporting signal organizations. DODIN operations personnel identify and maintain status of configuration items they operationally manage in the configuration management database. When a brigade is task-organized under a corps, division, or ARFOR, the brigade S-6 provides configuration item information to the joint chain of command and the theater army. Echelons brigade and below record all configuration management actions to systems they operationally manage in the configuration management database.

3-69. Corps and division G-6 section personnel manage configurations within the corps and division areas of operations, assisted by their organic signal, intelligence, and sustainment companies, supporting ESBs, and other supporting signal organizations. DODIN operations personnel identify and maintain status of configuration items they operationally manage in the configuration management database. The G-6 provides this information to Army forces in the area of operations, and to the theater army as the corps or division deploys. The corps, division, and subordinate units also record all configuration management actions to systems they operationally manage in the configuration management database.

3-70. The ESB performs configuration management for its supported tactical organizations. ESBs ensure configuration items they operationally manage, along with those of their supported organizations, reflect accurately in the configuration management database. The theater army provides this information to various tactical echelons as the ESB is task reorganized.

3-71. The SC(T) and RCC manage the configuration of the theater army's tactical support services. DODIN operations personnel identify and maintain status of configuration items they operationally manage in the configuration management database. The theater army also records all change management actions to systems they operationally manage in the configuration management database.

3-72. A unit may be responsible for a physical configuration item but not the device configuration. For example, a brigade enters its routers into, or removes them from, the configuration management database, while the brigade's higher headquarters, as the echelon that operationally manages the brigade's routers, maintains the router's configuration status in the configuration management database.

Configuration Management—Joint Implications

3-73. Joint guidance governs joint configuration management. Army units supporting these organizations operate according to joint guidance, while also following Army configuration management procedures as much as possible. Army DODIN operations facilities within these organizations use the Army-provided configuration management database unless otherwise directed. Joint organizations can view information from this database, as required.

3-74. J-6, The G-6, supporting ESB, and other supporting signal organizations manage configurations within their areas of operations and the joint operations area. Personnel supporting Army DODIN operations organizations identify and maintain configuration items they operationally manage in the configuration management database. The ARFOR G-6 verifies the accuracy of all changes to systems they operationally manage, and those of subordinate Army elements, in the configuration management database.

INCIDENT AND PROBLEM MANAGEMENT

3-75. Incident and problem management involves processing and resolving events which are not part of the standard operation of a DODIN operations capability, and which may interrupt or reduce the quality of that capability. The goal of incident and problem management is identifying the cause of an incident, taking deliberate measures to mitigate any vulnerability, and restoring the capability. Incident and problem management may feed the change management and configuration management processes. Synchronizing incident and problem management with change management and configuration management reduces adverse impacts on tactical operations to maintain the best possible quality, availability, and security. Army and joint signal staffs at all echelons manage network-related incidents and problems relating to user systems and capabilities. Incident and problem management includes responses to realign or reconstitute capabilities due to degraded and denied operating environments or changes in the operational or mission variables.

Incident and Problem Management—Echelons and Organizations

3-76. The S-6 and the brigade signal company perform incident and problem management for the BCT and below. When DODIN operations personnel identify an incident at the BCT, they analyze it to decide whether it can be resolved locally. In echelons BCT and below, the local ability to analyze incidents is very limited. If personnel cannot identify a solution locally, they escalate the problem to the next higher headquarters.

3-77. The G-6 and the corps or division signal, intelligence, and sustainment company conduct incident and problem management at the corps and division. When DODIN operations personnel identify an incident at the corps or division, or a subordinate organization escalates an unresolved incident to the corps or division, they analyze it to decide whether it can be resolved locally. If they cannot identify a local solution, they escalate the problem to the next higher headquarters.

3-78. The theater army performs incident and problem management for all DODIN operations capabilities they provide. If the theater army cannot resolve a tactical incident or problem through local resources, they may escalate the problem to the TNCC, material developer, or vendor subject matter experts.

Incident and Problem Management—Joint Implications

3-79. The ARFOR G-6 and supporting signal organizations perform incident and problem management within their operational areas. When DODIN operations personnel identify an incident, or a subordinate organization escalates an unresolved incident to the ARFOR G-6, they analyze it to decide whether it can be resolved locally. If DODIN operations personnel cannot find a local solution, they escalate the problem to the RCC or the joint network operations control center.

3-80. Joint guidance governs joint task force incident and problem management. Army personnel supporting these organizations operate according to joint guidance, while also following Army incident and problem management procedures as much as possible.

RELEASE MANAGEMENT

3-81. Release management includes planning, designing, constructing, configuring, and testing hardware and software to create a set of release components for a live environment. Release management also includes planning, preparing, and scheduling software releases to various subscribers and locations.

3-82. NETCOM initiates, plans, and tests most software releases for the Army. It is critical that NETCOM build and test these releases with the tactical environment in mind. This section provides details about those activities specific to the tactical echelons—release rollout planning, installation, and training.

3-83. Release planning follows the change management and planning processes. Change requests are the first step in release issue. The chain of command and all affected organizations coordinate and plan requested changes.

3-84. Release installation follows change management guidelines. The echelon responsible for change management of the affected system(s) executes the release.

SERVICE DESK MANAGEMENT

3-85. Tactical service desk management encompasses interfacing with tactical subscribers. Service desk management includes incident and problem processing, change request processing, availability management, user interaction, and collecting user satisfaction data.

3-86. The unit's signal staff and information systems management officers conduct service desk management for user systems and maintain local DODIN operations capabilities. The signal staff may assign service desk functions to a supporting signal unit, such as a signal company or ESB, as necessary.

Service Desk Management—Echelons and Organizations

3-87. At brigade and below, service desk management supports local subscribers. Service desk personnel collect and analyze information, and provide it to the G-6 or J-6 at the next higher echelon.

3-88. Personnel that perform service desk management at brigade and below are likely to be network design, engineering, or incident management personnel who are assigned additional duties for service desk management. At the division and higher, the table of organization and equipment includes authorized staffing for service desk personnel.

3-89. The theater army performs service desk management for all SC(T) or RCC tactical support services. They also provide service desk information to tactical Army units and the joint task force.

SERVICE DESK MANAGEMENT—JOINT IMPLICATIONS

3-90. Within the ARFOR headquarters, the G-6 and the supporting signal organizations manage the service desk. Joint guidance governs service desk management in a joint task force. Army personnel supporting these organizations operate according to joint guidance while also adhering to Army service desk procedures as much as possible.

INFRASTRUCTURE MONITORING AND MANAGEMENT

3-91. DODIN operations infrastructure monitoring is the continuous tracking of the IT components that provide DODIN operations capabilities. Monitoring focuses on the health of DODIN operations capabilities. Some of these capabilities are—

- Networked IP tactical radios.
- Multiplexers.
- Cryptographic devices.
- Routers.
- Switches.
- Firewalls.
- Intrusion detection systems.
- Enabling protocols.
- Host Based Security System.
- Critical applications.

3-92. DODIN operations personnel monitor infrastructure continuously. Monitoring supports and enables other DODIN operations activities, such as DODIN operations shared situational understanding, service desk management, and incident and problem management.

3-93. DODIN operations organizations conduct distributed infrastructure monitoring because of the complexity of DODIN operations infrastructure. Distributed monitoring systems collect critical information and forward it to higher-level DODIN operations monitoring systems. Distinct monitoring domains, aligned with the theater army's DODIN operations organizations, facilitate distributed monitoring. The theater army, corps, division, brigade, and battalion monitor their respective domains, as established in the DODIN operations mission plan.

3-94. Each organization's monitoring domain consists of the IT components in their area of operations and the status of the WAN links to their directly higher and subordinate organizations. For example, a corps or division monitoring domain consists of all the IT components in its area of operations, as well as the WAN links to the theater army or joint task force (higher organization), adjacent units, ESBs, and its BCTs and functional brigades (subordinate organizations). In most cases, line of sight and other WAN connections in a unit's monitoring domain provide connectivity to remote elements of the unit. In this situation, the unit monitors all IT components connected via WAN links.

3-95. In a deployed scenario, there may be ad hoc Army, joint, inter-organizational, and multinational assets attached to a brigade, corps, or division. When this occurs, the supported command monitors the attached assets. If an attached unit, such as an ESB or Marine expeditionary force, is capable of independent monitoring, this unit forwards their monitoring data to the supported command. If not, the supported command assumes active, near real-time monitoring of the attached unit.

3-96. Tactical units also need some visibility of adjacent and higher networks for situational understanding and troubleshooting. Higher echelons provide a high-level view of the network via remote network views.

INFRASTRUCTURE MONITORING AND MANAGEMENT—ECHELONS AND ORGANIZATIONS

3-97. For the BCT and battalion, the S-6 and brigade signal company monitor the network infrastructure. These organizations use their DODIN operations monitoring systems to monitor, manage, and troubleshoot the network infrastructure in their area of operations. The battalion provides event and alarm data and network topology from its area of operations to the BCT. This data provides the BCT a read-only view of the battalion's infrastructure for troubleshooting and analysis.

3-98. The BCT provides all monitoring information from its area of operations to the corps and division DODIN operations monitoring systems. This information consists of event and alarm data, and network topology. This provides the corps and division a read-only view of the BCT and battalion infrastructure for troubleshooting and analysis.

3-99. The G-6 and supporting signal organizations monitor network infrastructure within the corps and division. The corps and division use their DODIN operations monitoring systems to monitor, manage, and troubleshoot the network infrastructure within their area of operations. The corps and division provide all monitoring information from their area of operations, including subordinate BCT and battalion information, to the theater army or joint task force DODIN operations monitoring system. This information, consisting of event and alarm data and network topology, provides the higher headquarters a read-only view of the network infrastructure for troubleshooting and analysis. The corps and division also provide consolidated DODIN operations monitoring information to subordinate units for situational understanding and troubleshooting.

3-100. The RCC uses its DODIN operations monitoring system to monitor, manage, and troubleshoot the network infrastructure within the theater on behalf of the theater army. The RCC also provides theater-wide monitoring information to the TNCC and subordinate Army organizations within the theater for situational understanding and troubleshooting.

INFRASTRUCTURE MONITORING AND MANAGEMENT—JOINT IMPLICATIONS

3-101. The ARFOR G-6 manages DODIN operations capabilities and infrastructure within its area of operations through its subordinate corps, divisions, brigades, and other domains' monitoring and management activities. The ARFOR G-6 provides all event and alarm data and network topology from its subordinate organizations to the theater army's DODIN operations monitoring system. The ARFOR G-6 also provides consolidated monitoring and management information to subordinate elements for situational understanding and troubleshooting. According to joint guidance, the joint task force directs DODIN operations monitoring and management within the joint operations area. Army organizations supporting joint commands monitor and manage according to the processes listed above, unless these processes conflict with joint guidance. The ARFOR G-6 adjudicates conflicts between joint guidance and Army requirements.

PHYSICAL AND OPERATIONAL MANAGEMENT

3-102. Physical and operational management are two distinct, but complementary, DODIN operations activities. Physical management of a DODIN operations system, capability, or component involves day-to-day activities to keep the system, capability, or component running. These activities include providing power, environmental controls, cleaning, preventive maintenance, installation and de-installation, physical inventory, and hands-on labor. Operational management includes configuration, reconfiguration, monitoring, patching, and upgrading. Some of the devices are computing platforms, routers, switches, multiplexers, uninterruptible power supplies, encryption devices, and intrusion detection systems.

3-103. Global policy and network topology define physical and operational management responsibilities. The interconnection of IP networks is hierarchical, though the transmission system is relatively flat. The demarcation points between network tiers and tactical unit boundaries are natural borders for physical and operational management. The unit that physically controls an item usually exercises physical management. Operational management of DODIN operations capabilities, systems, and components falls into the following three categories—

- **Unit-managed component systems.** The echelon that physically controls components or systems that cannot be remotely managed (for instance, a squad-level radio) operationally manages those components or systems.
- **Theater-level capabilities.** Theater signal organizations manage and operate some systems as theater-level capabilities. These systems are designed and implemented to provide flexible capabilities. They do not need frequent reconfiguration to meet tactical requirements. Some examples of theater-level capabilities include the Army domain name service and the joint router network. The echelon at which these capabilities reside also operationally manages these systems.
- **Echelons above brigade managed systems.** The remaining DODIN operations capabilities, systems, and components are both remotely manageable and need distributed management to align with command requirements. The next higher echelon operationally manages these systems in a brigade. This echelon is usually a division, though in some scenarios the echelon above brigade may be a corps, theater army, or joint command. Some examples of systems managed above brigade are unified communications managers, voice over IP gateways, private branch exchanges, routers, firewalls, collaboration tools, and unit directory services. NETCOM may manage some of these systems as enterprise-level capabilities.

Note. Any echelon with operational management responsibilities may delegate responsibility to subordinate echelons or organizations, as needed.

Physical and Operational Management—Echelons and Organizations

3-104. All echelons execute physical and operational management. The component types in the DODIN operations infrastructure are the same, regardless of where they reside in a theater army, corps, division, brigade, or battalion. These include, but are not limited to, routers, data switches, voice switches, private branch exchanges, multiplexers, satellite communications terminals, line of sight transmission equipment, and computing platforms. Location and ownership of DODIN operations capabilities, systems, or components often affects which echelon or organization exercises physical management. For example, a corps or division operates and manages unit-managed radios in the corps or division signal, intelligence, and sustainment company. The brigade manages the same type radios in the brigade signal company.

3-105. The theater army operationally manages capabilities, systems, and components for Army forces across the entire theater. The RCC executes physical and operational management to support the theater army G-6 and SC(T). Besides managing and operating capabilities, systems, and components for its portion of the DODIN operations infrastructure, the RCC operates and manages theater support services. Some of these capabilities include Army domain name service, intrusion detection system, and tier-1 routing domains.

3-106. The deployment of intrusion detection system to an organization is a good example to illustrate physical and operational management responsibilities for interdependent devices across multiple organizations. In this example, an organization receives an intrusion detection system pre-configured with an IP address. The receiving organization could be a corps, division, brigade, or a battalion. Several organizations perform physical and operational management activities on various devices to deploy the intrusion detection capability. The receiving organization configures the intrusion detection system and connects it to the IP network (operational activity). When installed, the intrusion detection system is immediately active on the local area network. The local organization may need to create a reservation in their Dynamic Host Configuration Protocol server (manage Dynamic Host Configuration Protocol activity) and reconfigure local firewalls to allow the protocols and IP address of the intrusion detection system (manage firewall activity). The RCC reconfigures its firewalls and intrusion detection system management station to complete the deployment.

Physical and Operational Management—Joint Implications

3-107. The ARFOR commander delegates responsibility for operating and managing capabilities, systems, or components within their area of operations to corps, divisions, and directly reporting brigades, as appropriate. The theater army controls and manages Army force components OPCON to support a joint task force. The RCC executes control and management to support the theater army G-6 and SC(T). The joint task force coordinates operation and management of joint DODIN operations capabilities, systems, and components.

SECURITY MANAGEMENT

3-108. Security management is part of, and included in, each DODIN operations activity. This section focuses on security-specific functions that support other DODIN operations activities.

3-109. DODIN operations security management includes the cybersecurity activities that serve to protect information and information systems by ensuring their confidentiality, integrity, availability, authentication, and nonrepudiation. Many cybersecurity capabilities are Army-wide enterprise capabilities. For example, Microsoft Windows Active Directory provides enterprise-wide identity and access management for Windows platforms.

3-110. Defense-in-depth is fundamental to security of the DODIN. Defense-in-depth identifies three network-accessible areas that require protection—

- **Perimeter defense** includes protection for both public and extranet access. Extranet access includes those ports and protocols external to, and specifically identified by, the tactical unit. An extranet is a private network that uses IP and the public telecommunications system to share information securely among selected external users. An extranet requires firewalls, authentication, encryption, and virtual private networks that tunnel through the public network (refer to AR 25-2).
- **Enclaves** are usually contiguous networks that support specific geographic locations, organizations, or units.
- **Hosts** are the final layer of defense. Protection at this layer consists of host-based configuration parameters and host-based intrusion detection and prevention software.

3-111. Information management security tools support event collection, data reduction, and correlation to support these defensive components.

SECURITY MANAGEMENT—ECHELONS AND ORGANIZATIONS

3-112. Centralized security management ensures consistency and reduces the number of specialized personnel needed to analyze network security. Cybersecurity personnel manage network security in near real-time to increase effectiveness. Security management includes near real-time, uninterrupted physical and operational management of network security components and sensors. The RCC may use information management security tools to aggregate and analyze DODIN operations event information in support of tactical organizations.

3-113. The RCC centrally manages perimeter protection components and sensors within the theater. The operating tempo may necessitate support from the RCC's deployment support division to meet deployed commanders' network security needs.

3-114. The RCC also manages enclave protection components and sensors. The RCC may delegate this responsibility to corps, division, or brigade level organizations, at the discretion of the operational chain of command. The corps, division, and brigade also manage enclave protection if they lose connectivity to the RCC.

3-115. Local commanders at all levels conduct host protection. ESB and signal company personnel help local commanders, as requested or directed.

SECURITY MANAGEMENT—JOINT IMPLICATIONS

3-116. Joint guidance governs joint task force security management. Army personnel supporting joint task forces operate within this guidance, while also following Army security management procedures as much as possible.

3-117. Within the joint task force, the J-6, Army component G-6 or S-6, and the supporting signal organizations manage network security. When the ARFOR G-6 identifies a potential security incident, or a subordinate organization escalates an incident to the ARFOR headquarters, the G-6 identifies the incident's potential local impact and escalates the incident to the joint network operations control center. The operational chain of command directs appropriate responses or defensive measures.

CAPABILITY EVALUATION

3-118. Within the operational environment, DODIN operations personnel evaluate DODIN operations capabilities to ensure they achieve their intended goals. Evaluation focuses on the health and protection of these capabilities. Evaluation activities fall into two areas: cybersecurity compliance and DODIN operations capacity and availability.

3-119. A DODIN operations capability must meet specific requirements to perform its intended function. These requirements are characterized by key parameters which, when evaluated against thresholds, provide useful information about the capability's health. For example, a key parameter of a T-1 circuit is the transmission rate. If the traffic load exceeds the maximum transmission rate threshold of 1.536 megabits per second, users can expect dropped packets or slowed application performance (degraded availability).

3-120. Capability evaluation helps identify degraded availability, capacity shortfalls, and cybersecurity noncompliance. Evaluation activities provide information required for capability planners, cybersecurity analysts, and engineers to apply remediation or isolation actions, reallocate resources, and identify DODIN operations capability upgrades to ensure the continued availability of network services. *Remediation* is the act of mitigating a vulnerability or a threat (CNSSI 4009).

3-121. Evaluation activities focus on the health, maintenance, and protection of DODIN operations capabilities. Evaluating long-term trends provides information on the overall health of the DODIN operations systems. Trend evaluation may illuminate training deficiencies or weaknesses in individual components or systems. It also provides valuable information to evaluate the effectiveness of doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy.

3-122. Capability evaluation supports capacity, availability, and cybersecurity compliance monitoring and reporting. It focuses on the health and protection of the network and its services and supports proactive DODIN operations.

CYBERSECURITY COMPLIANCE

3-123. Cybersecurity compliance requires vulnerability assessments. Cybersecurity compliance evaluation entails maintaining systems, identifying deficiencies, and recording results in the configuration management database. These assessments ensure prompt and adequate vulnerability remediation. Regularly scheduled evaluation is part of the overall cybersecurity plan. Some DODIN operations capabilities requiring cybersecurity compliance are—computing platforms, client applications, server applications, routers, and data switches that provide network capabilities.

CYBERSECURITY COMPLIANCE—ECHELONS AND ORGANIZATIONS

3-124. The RCC provides IAVM messages for distribution to theater teams and NECs. The NECs ensure corps, divisions, and brigades comply with cybersecurity updates. Units must report IAVM and information assurance (IA) vulnerability bulletin compliance in the Army Cyber Vulnerability Tracking databases. The RCC pushes updates to organizations that exercise operational management for action. The corps and division G-6 maintain situational awareness of units in the AOR and decide when to apply IAVM updates. In some instances, a DODIN operations capability has many baseline configurations. In this situation, the tactical operations staff modifies, recreates, and tests IAVM updates before distributing them. IAVM compliance is mandatory and is a command responsibility.

> ***Note.*** Although cybersecurity formally replaced the term information assurance across the DOD, certain duty positions, processes, and websites retain IA in their proper titles.

3-125. The corps and division G-6 maintain cybersecurity compliance according to the commander's intent. The G-6 uses the appropriate resources to accomplish this mission. The organization that operationally manages a system ensures cybersecurity compliance for that system. The variety and complexity of DODIN operations capabilities may require specialized groups to operate and maintain the systems. For instance, the signal company is the best location to apply a compliance package for a telecommunications component. Determining which organization performs the compliance activity depends on where the component is located and which organization exercises operational management. In another instance, the corps or division sanctuary is the appropriate location to modify and apply a patch for a computing platform. The organization with physical or operational management is responsible for reporting compliance to the corps or division G-6, via the signal company, or the corps or division sanctuary. The theater army compiles compliance reports from the corps and division G-6.

CYBERSECURITY COMPLIANCE—JOINT IMPLICATIONS

3-126. The ARFOR G-6 maintains cybersecurity compliance in its area of operations, according to the commander's intent. The G-6 uses the appropriate resources to accomplish this mission.

3-127. The theater army evaluates cybersecurity compliance of the Army force component of a joint task force. The joint task force coordinates cybersecurity compliance evaluation for DODIN operations capabilities, systems, and components in the joint operations area.

CAPACITY AND AVAILABILITY

3-128. DODIN operations infrastructure capacity correlates with availability of DODIN operations capabilities. While the functions are different, the organizational responsibilities are the same. Infrastructure monitoring allows planners to ensure continued adequate DODIN operations capacity and availability. Infrastructure monitoring is a short-term activity that supports long-term planning for IT capacity and availability.

3-129. DODIN operations capacity evaluation ensures effective network services and applications to support the Soldier, and efficient use of DODIN operations capabilities. Evaluation results aid planners in forecasting capability degradation and allow them to recommend capability reallocation and upgrades to maintain the health and protection of the DODIN operations infrastructure. Capacity evaluation provides critical information for infrastructure planners to proactively allocate resources and identify potential bottlenecks. DODIN operations personnel compare key operating parameters of networking equipment, computing platforms, peripherals, and software to threshold metrics to identify potential capacity shortfalls.

3-130. The purpose of availability evaluation is to ensure sustained availability, reliability, and maintainability of DODIN operations capabilities. As in capacity evaluation, DODIN operations personnel compare key operating parameters of networking equipment, computing platforms, peripherals, and software to threshold metrics to identify potential shortfalls. DODIN operations capability planners use the results to improve the overall availability of the capabilities, ultimately reducing the frequency and duration of adverse incidents.

CAPACITY AND AVAILABILITY—ECHELONS AND ORGANIZATIONS

3-131. The corps and division G-6 monitor systems they control to evaluate the capacity and availability of DODIN operations capabilities and enabling devices. They also evaluate the capacity and availability of subordinate brigades to assess the overall DODIN operations capacity and availability in their area of operations. They report the total capacity and availability evaluations to the theater army.

3-132. The theater army evaluates the capacity and availability of their DODIN operations capabilities and enabling devices, along with those from other service providers such as the Defense Information Systems Agency. They use the results of their evaluations to improve capacity and availability locally and at other DODIN operations facilities. The theater army evaluates capabilities across the entire theater, based on capacity and availability evaluations from lower echelons. This evaluation helps to formulate an appropriately-scoped assessment, and allows them to detect issues they might overlook using a narrower view from a lower echelon.

3-133. DODIN operations personnel at all echelons improve the capacity and availability of the DODIN operations infrastructure through the change management process. The change management process ensures proper coordination to help achieve the overarching goal of improved efficiency.

Capacity and Availability—Joint Implications

3-134. The ARFOR G-6 evaluates capacity and availability of the DODIN operations capabilities and enabling devices under its control. The ARFOR G-6 also directs capacity and availability evaluation within the corps, division, brigades, ESBs, and other subordinate signal organizations to form an assessment scoped to its area of operations. The ARFOR G-6 reports these evaluations to the theater army. The ARFOR G-6 also evaluates and reports capacity and availability to its joint command J-6, as directed by joint policy.

TRAINING AND EXERCISE

3-135. Effectively employing DODIN operations capabilities requires continuous training. As new or updated capabilities enter the tactical environment, Soldiers' skills need enhancement or refreshment.

3-136. As the network's capabilities and dependencies evolve, DODIN operations increase in complexity. DODIN operations span the entire enterprise, rather than being limited to a local network, a small enclave, a tactical battlefield, or the strategic environment. Soldiers rely on the continuous network availability these capabilities enable. DODIN operations capabilities depend on the proper mix of equipment and processes, properly used by technically competent personnel.

3-137. DODIN operations activities have multiple impacts. First, they expose many of the challenges that tools, technologies, and processes address to leverage the enterprise as a force multiplier. Second, they open communications and expose expertise and capabilities to leverage them across the enterprise. The continuous exercise of DODIN operations activities improves organizations' understanding of the capabilities, challenges, and expertise required at each echelon to maintain effective enterprise DODIN operations.

3-138. Soldiers train in the same activities they perform when deployed. The training environment replicates, as closely as possible, the conditions, circumstances, and influences of the operational environment, regardless of the training location. Simulators or simulations may augment DODIN operations training.

Training and Exercise—Echelons and Organizations

3-139. Soldiers train and practice individual and collective tasks based on their mission, doctrine, and the unit task list. Organizing collective tasks into task selections enables efficient collective training, using a methodology appropriate to the echelon and Soldiers' experience. Training builds from the individual and team task level through company, battalion, brigade, and higher-level exercises.

Training and Exercise—Joint Implications

3-140. The Army must be ready to execute its mission as part of a joint force. To achieve this goal, Army forces train with joint, inter-organizational, and multinational elements to prepare for joint missions.

3-141. Joint interoperability is an essential part of training requirements, from individual and collective training at Army learning centers, through integrated command post exercises. Joint interoperability training is part of the Combined Arms Training Strategy for signal units. Joint interoperability training improves units' readiness to perform the interdependent activities and organizational relationships for joint operations. It also simplifies Army units' integration into the joint enterprise and adherence to joint network operations standards and doctrine.

INTERRELATIONSHIP OF DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS ACTIVITIES

3-142. Success in DODIN operations requires close coordination and cooperation within and between responsible organizations at all echelons. The activities described in this chapter are both interrelated and interdependent. For example, incident and problem management rely on change management to implement corrective actions. These activities also rely on infrastructure monitoring to detect anomalies.

SUPPORT TO DEFENSIVE CYBERSPACE OPERATIONS

3-143. DODIN operations protection measures—specifically cybersecurity—are network-focused and not specific to a particular threat, while defensive cyberspace operations are mission-focused and threat specific. Cybersecurity sets the baseline security posture of the network. Defensive cyberspace operations entail deliberate measures to counter specific threat actions. Cybersecurity compliance activities support defensive cyberspace operations; the goal of both is a secure network.

3-144. Cybersecurity and defensive cyberspace operations share a mutually supporting relationship. Determining which is the main effort and which is the supporting effort depends on intent, focus, and the current situation. For example, if an adversary cyberspace attack is identified or anticipated, defensive cyberspace operations will be the main effort, with cybersecurity supporting.

3-145. In case of DODIN security compromise, network defenders implement prompt and comprehensive defensive cyberspace operations-internal defensive measures to counter and defeat the threat, mitigate its effects, and restore network security. DODIN operations personnel perform those internal defensive measures they can within the defended network.

3-146. Some security compromises need special outside investigation and threat search capabilities to mitigate the threat. DODIN operations personnel enable these efforts by strictly adhering to cybersecurity standards. For more information about defensive cyberspace operations-internal defensive measures, see FM 3-12.

SUPPORT TO OFFENSIVE CYBERSPACE OPERATIONS AND DEFENSIVE CYBERSPACE OPERATIONS-RESPONSE ACTIONS

3-147. Offensive cyberspace operations and defensive cyberspace operations-response actions create effects outside of U.S. or other friendly cyberspace. *Defensive cyberspace operations-response actions* are operations that are part of a defensive cyberspace operations mission that are taken external to the defended network or portion of cyberspace without the permission of the owner of the affected system (JP 3-12). These operations may use friendly networks to plan and launch attacks. The systems used for these missions implement the most stringent cybersecurity measures, and normally only connect to the friendly network at the time of execution. For more information about cyberspace operations, see FM 3-12.

CYBERSPACE ELECTROMAGNETIC ACTIVITIES

3-148. Signal planners face the challenge of determining how to enable joint, inter-organizational, and multinational partner collaboration and assure access to critical data and information networks in increasingly contested and congested cyberspace and electromagnetic operational environments, while simultaneously denying the same to the enemy. For this reason, DODIN operations planning requires collaboration and coordination through cyberspace electromagnetic activities. *Cyberspace electromagnetic activities* are the process of planning, integrating, and synchronizing cyberspace and electronic warfare operations in support of unified land operations (ADRP 3-0). Cyberspace electromagnetic activities synchronize—

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

3-149. Each of the signal, cyberspace, and electronic warfare missions shares certain areas of potential overlap with one or more of the others. Each has its own set of threat and performance indicators. Closely collaborating and synchronizing signal, cyberspace, and electronic warfare missions and tasks strengthens all of them beyond their inherent capabilities. Shared awareness between signal, cyberspace operations, electronic warfare, and intelligence elements improves situational understanding and identifies opportunities for mutual support between the capabilities. Coordinating spectrum use between signal and electronic warfare elements ensures these missions do not interfere with one another in the electromagnetic spectrum. Failing to share situational understanding could cause planners or operations personnel to miss indicators of a cyberspace or electronic attack or lead to unintended consequences when conducting operations.

3-150. Synchronizing signal, cyberspace, electronic warfare, and intelligence capabilities is especially important when planning for or operating against a peer threat. An enemy can use radio frequency direction finding equipment to locate any radio frequency emitter, such as a radio, satellite communications terminal, counter-improvised explosive device system, radar, or cell phone. Once they determine an accurate location, the enemy can direct lethal fires to destroy the capability.

3-151. Combining signal and electronic protection techniques with current intelligence estimates may mitigate an adversary's ability to locate and attack key communications nodes or command posts. The intelligence section can better define an enemy's electronic order of battle. The electronic warfare officer's knowledge of electronic warfare threats and techniques helps inform a communications plan to limit the enemy's effectiveness. Some of the planning factors may include—

- Formulate network plans to minimize the electromagnetic signature.
- Use low probability of detection and low probability of intercept modulation techniques.
- Accurately identify real communications requirements—lower date rates require less radio frequency power.
- Emission control (limiting radio transmissions).
  - Transmit only when necessary.
  - Limit the duration of transmissions.
- Locate large communications nodes and radars as far from the command post as practical.

Note. For more information about cyberspace electromagnetic activities, see FM 3-12. For more information about electronic warfare, see JP 3-13.1, FM 3-12, and ATP 3-36. For more information about spectrum management operations, see ATP 6-02.70.

Appendix A

Department of Defense Information Network Operations Components

Department of Defense information network operations consist of enterprise management, cybersecurity, content management, network situational understanding, and their underlying principles and components. This appendix discusses the components of Department of Defense information network operations, and discusses and defines each essential task and component, and their relationships with the other components.

DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS OPERATIONAL CONSTRUCT

A-1. DODIN enterprise management, DODIN content management, cybersecurity, and network situational understanding guide the installation, management, and protection of communications networks and information services to support operational forces. DODIN operations provide users and systems at all levels with end-to-end network and information system availability, information protection, and prompt information delivery. Figure A-1 on page A-2 depicts how Army DODIN operations tasks nest within, and correspond with, the wider joint DODIN operations functions. Network management and enterprise systems management (DODIN enterprise management) consist of steps to configure, assign, process, connect, route, flow, account for, and maintain network capabilities. Information dissemination management and content staging (DODIN content management) allow users to retrieve, cache, compile, catalog, and distribute information to support planning and decision making. Cybersecurity provides the means to resist and recognize intrusions and to recover and reconstitute network capabilities. The net effect of integrating the three tasks is information advantage. The right user gets the right information at the right time, with the right protection and in a usable format.

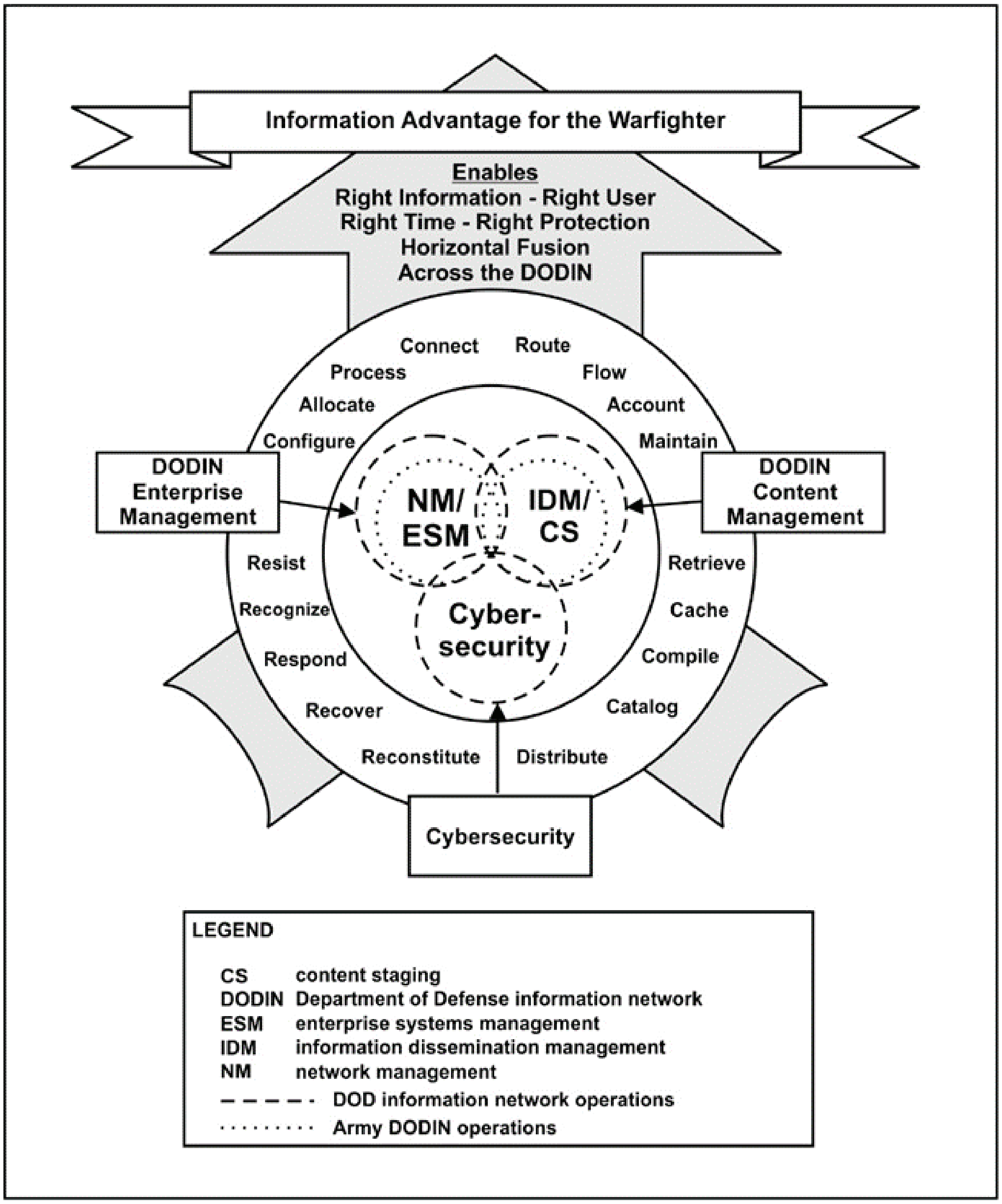

Information Advantage for the Warfighter
Enables
Right Information - Right User
Right Time - Right Protection
Horizontal Fusion
Across the DODIN
Connect
Route
Process
Flow
Allocate
Account
Configure
Maintain
DODIN Enterprise Management
DODIN Content Management
NM/ ESM
IDM/ CS
Cyber- security
Resist
Retrieve
Recognize
Cache
Respond
Compile
Recover
Catalog
Reconstitute
Distribute
Cybersecurity
LEGEND
CS content staging
DODIN Department of Defense information network
ESM enterprise systems management
IDM information dissemination management
NM network management
– – – – DOD information network operations
········· Army DODIN operations

Figure A-1. Department of Defense information network operations operational construct

DEPARTMENT OF DEFENSE INFORMATION NETWORK ENTERPRISE MANAGEMENT

A-2. DODIN enterprise management is the technology, processes, and policies necessary to effectively and efficiently install, operate, maintain, and sustain communications networks, information systems, and applications. DODIN enterprise management merges IT services with DODIN operations critical capabilities.

Functional Services

A-3. The five major functional services of DODIN enterprise management foster the installation, operation, maintenance, and sustainment of communications networks and information services technologies to ensure their performance, availability, and security. These services are inherent at the strategic, operational, and tactical levels across all warfighting functions. The five functional services are—

- **Enterprise systems management** for end-user and system applications focuses on the availability, performance, and responsiveness of enterprise service capabilities. Enterprise services are IT services that span an entire large organization, or enterprise. In the case of the DODIN, enterprise refers to the DOD, including all of its organizational entities (DODD 8115.01). Some enterprise services are—
  - DOD Enterprise E-mail.
  - DOD Enterprise Portal Service.
  - Defense Collaboration Services.
  - Enterprise search.
  - Enterprise file share.
  - Identity and access management.
- **Systems management** provides day-to-day administration of computer-based systems, elements of systems, and services including software applications, operating systems, databases, and hosts of end-users. Systems management is comprised of all measures necessary to operate enterprise systems and services effectively and efficiently.
- **Network management** provides a network infrastructure with the desired level of quality and guaranteed service. Networks included in enterprise management are located on all transmission media and tiers of communication: terrestrial, aerial, and satellite communications. They include digital telephony, packet routing, and cell-switched networks using fiber optic or wireless transport media.
- **Satellite communications management** is the day-to-day operational control of satellite communications resources. In the Army, the operational authority for satellite communications management is United States Army Space and Missile Defense Command/Army Forces Strategic Command. See FM 3-14 and ATP 6-02.54 for more information about satellite communications management. Satellite communications management includes—
  - Appropriate support when service is disrupted.
  - Providing satellite communications system status.
  - Maintaining situational understanding, including current and planned operations, as well as space, control, and earth segment asset and operational configuration management.
  - Satellite anomaly resolution and management.
  - Satellite communications interference to the network.
- **Frequency assignment** involves ensuring frequency resources are available to support effective and efficient frequency use for planning, managing, and operating the wireless portion of the network. Ensuring frequency availability requires determining accurate spectrum requirements and coordinating with spectrum managers, who continually deconflict frequencies used for the network, enabling dynamic operations. The frequency assignment function of spectrum management operations enables frequency availability. In the Army, the operational authority for frequency assignment is the Army Spectrum Management Office. See ATP 6-02.70 for more information about spectrum management operations.

Critical Capabilities

A-4. DODIN enterprise management involves several critical capabilities associated with IT services. Enterprise managers must achieve these capabilities at the strategic, operational, and tactical levels across all warfighting functions. Enterprise management has five critical capabilities—

- **Fault management** is associated with failure of the network or information systems that affects connectivity and functionality. Fault management is a five-step process:

  - Detect faults.
  - Locate faults.
  - Restore service.
  - Identify the cause of the fault.
  - Establish solutions so similar faults do not occur in the future.
- **Configuration management** applies technical and administrative direction and surveillance to—
  - Identify and document the functional and physical characteristics of a configuration item.
  - Control changes to those characteristics.
  - Record and report changes to processing and implementation status.
- **Accounting management** helps effectively allocate internal and external resources. The goal of accounting management is to identify true requirements based on network monitoring and system use. The desired result is a network and information systems configuration that provides the most effective, efficient use of resources. Planners also use monitoring data to identify future resource requirements.
- **Performance management** is monitoring and managing network and information systems performance. Performance management involves—
  - Data monitoring.
  - Problem isolation.
  - Performance tuning.
  - Statistical analysis for trend recognition.
  - Resource planning.
- **Security management** is implementing technical and administrative measures to secure access to the information transmitted over the network or processed and stored on information systems. Security management integrates enterprise management with cybersecurity.

Enabled Effects

A-5. DODIN enterprise management enables network and information system availability and information delivery. These effects are achieved by—

- Maintaining robust network capabilities in the face of component or system failure or adversary attack.
- Configuring and allocating network and information system resources.
- Rapidly and flexibly deploying network resources.
- Ensuring effective, efficient, and prompt processing.
- Ensuring connectivity, routing, and information flow.
- Planning for increased network use.

Objective

A-6. The objective of DODIN enterprise management is to provide network control for Army communications systems and enable interoperability with joint networks. Army DODIN operations managers conduct enterprise management at all levels of military operations.

Enterprise Management Activities

A-7. Specific enterprise management functions and tasks may vary, depending on the organization's mission and capabilities. All NOSCs share some common enterprise management activities. These activities occur during predeployment, deployment, and redeployment. Enterprise management consists of seven activities. Each activity is a different step in the enterprise management cycle. Each activity has associated network and information systems management resources identified to create controllable enterprise management. Each enterprise management activity involves specific functions and associated tasks, whether the activity applies to user communications networks, or to networks provided by support elements. These activities are—

- Physical and operational management.
- Service delivery.
- Service support.
- Mission planning.
- Capability design and engineering.
- Sustainment.
- Administration.

A-8. DODIN enterprise management supports the commander's information requirements via physical and operational management, service delivery, and service support. The enterprise management cycle begins at the beginning of the operations process. The cycle is a continual process of identifying requirements (plan), determining courses of action (prepare), and execution (execute), with assessment integrated at every step. For more information about operational planning, see ADRP 5-0.

A-9. Mission planning, and capability design and engineering, are centralized activities that design networks to meet users' service requirements. Sustainment support is required to maintain existing services and acquire equipment to meet new service requirements.

Physical and Operational Management

A-10. Network managers provision services to add, delete, or change network and information system services available to users. Physical and operational management include the non-engineering tasks associated with allowing users to access requested services. Services may be global, such as the DODIN long-haul capability controlled and managed by the global enterprise operations center. Services may also be direct user services provided by a network manager at a NOSC, or at the theater or BCT level. Physical and operational management involve—

- Implementing configuration changes.
- Installing sub-elements.
- Verifying service modifications.
- Configuring end-user equipment.

Service Delivery

A-11. Service delivery involves directly interfacing with users to monitor satisfaction with the services provided by the network or information systems. Service delivery pertains to services required to support the Army mission areas (business, enterprise information environment, and warfighter). Service delivery involves—

- Managing service levels.
- Financially managing IT services.
- Managing capacity.
- Managing IT service continuity.
- Managing availability.

Service Support

A-12. Service support provides monitoring and control so that the network and systems continue to operate and provide quality service. Service support targets network and systems operations and management. DODIN operations managers conduct service support continuously. Service support involves—

- Service desk functions.
- Incident management.
- Problem management.
- Configuration management.

- Change management.
- Release management.

MISSION PLANNING

A-13. Mission planning is assessing user requirements and developing the schedule and resources to meet those requirements. Mission planning includes current, short-term (less than 2 years), and long-term (2–10 years) planning requirements. Mission planning ensures changing service requirements are collected, analyzed, prioritized, cost-assessed, and scheduled for implementation. The ultimate goal of mission planning is to ensure resources are available to meet current and future requirements, and that proposed implementations conform to subsequent short- and long-term objectives.

A-14. Mission planning involves—

- Analyzing user requirements.
- Assessing technology.
- Defining architecture.
- Planning and programming services.
- Defining and funding subsystems.
- Conducting cost-benefit analyses.
- Establishing performance objectives.
- Planning for contingencies and restoration.
- Planning system capacity.
- Planning system utilization.
- Planning systems and network integration.
- Planning security measures.
- Planning frequency assignments.
- Identifying satellite communications requirements and planning networks across satellite communications assets.

CAPABILITY DESIGN AND ENGINEERING

A-15. Capability design and engineering adapt the network and information system resources to meet user service requirements. Capability design and engineering base network and systems design on planning guidance and new service requirements. Capability design and engineering take place at all levels from global strategic enterprise management down to the theater army and regional cyber center. Capability design and engineering involve—

- Assisting users with planning.
- Designing networks and systems.
- Designing security infrastructure.
- Designing facilities and equipment.
- Integrating operations, facilities, and equipment.
- Developing technical documentation.
- Defining specifications for equipment and services.
- Defining implementation design and developing implementation procedures.
- Developing hardware and software.
- Developing and supporting information systems.
- Assigning frequencies.

SUSTAINMENT

A-16. The *sustainment warfighting function* is the related tasks and systems that provide support and services to ensure freedom of action, extend operational reach, and prolong endurance (ADP 3-0). The sustainment warfighting function includes (ADP 4-0)—

- Logistics.
- Maintenance.
- Transportation.
- Supply.
- Field services.
- Distribution.
- Operational contract support.
- General engineering support.
- Personnel services.
- Health service support.

ADMINISTRATION

A-17. Administration is associated with budgeting, training, procurement, staffing, and other business-related functions. Network managers perform these functions primarily at the strategic, sustaining base level and at theater bases, posts, camps, or stations. They perform some of these functions to a lesser degree at all levels of enterprise management. Administration activities involve—

- Training management.
- Program and budget management.
- Procurement.
- Staffing management.
- Chargeback.
- Special services.

CYBERSECURITY

A-18. The Army depends on reliable networks and systems to access critical information and supporting information services to accomplish their missions. Threats to the DODIN exploit the increased complexity and connectivity of Army information systems and place Army forces at risk. Like other operational risks, cyberspace risks affect mission accomplishment. They can increase the needed time and space to conduct operations, or decrease a unit's performance or effectiveness. DOD networks experience adversary cyberspace attacks every day. Robust cybersecurity measures prevent adversaries from accessing the DODIN through known vulnerabilities. The cybersecurity measures apply to general threats and known vulnerabilities, as opposed to specific attacks.

A-19. Cybersecurity ensures IT assets provide mission owners and operators confidence in the confidentiality, integrity, and availability of information systems and information, and their ability to make choices based on that confidence. The DOD cybersecurity framework (see DODI 8500.01) provides the foundation for cybersecurity.

A-20. Cybersecurity supports effective operations in cyberspace where—

- Missions and operations continue under any cyberspace threat situation or condition.
- IT components of weapons systems and other defense platforms function as designed and adequately meet operational requirements.
- The DODIN collectively, consistently, and effectively defends itself.
- The information network securely and seamlessly extends to mission partners.
- U.S. forces and mission partners can access their information and command and control channels, but their adversaries cannot.

A-21. DOD cybersecurity complies with National Institute of Standards and Technology security and risk management publications to ensure mission partner interoperability. These publications are available online at the National Institute of Standards and Technology Computer Security Resource Center.

A-22. The cybersecurity framework consists of—

- Cybersecurity risk management.
- Operational resilience.
- Integration and interoperability.
- Cyberspace defense.
- Cybersecurity performance.
- DOD information.
- Identity assurance.
- IT.
- Cybersecurity workforce.
- Mission partners.

CYBERSECURITY FUNDAMENTAL ATTRIBUTES

A-23. Cybersecurity ensures the confidentiality, integrity, availability, authentication, and nonrepudiation of friendly information and information systems while denying adversaries access to the same information and information systems. These attributes are—

- **Confidentiality** is assurance that sensitive information is not disclosed to unauthorized individuals, processes, or devices.
- **Integrity** is the reliability of an information system; the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. A formal security model defines integrity more narrowly to protect against unauthorized modification or destruction of information.
- **Availability** is timely, reliable access to data, and information services by authorized users.
- **Authentication** is a security measure designed to—
  - Protect a communications system against acceptance of a fraudulent transmission or simulation by establishing the validity of a transmission, message, or originator.
  - Provide a means of identifying individuals and verifying their eligibility to receive specific categories of information.
- **Nonrepudiation** is assurance that the sender of data receives proof of delivery and the recipient receives proof of the sender's identity to create a record of the parties that processed the data.

A-24. Cybersecurity incorporates those actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity on DOD information systems and computer networks. It incorporates protection, detection, and response while facilitating restoration of information systems. Cybersecurity provides end-to-end protection to ensure data quality and protection against unauthorized access and inadvertent damage or modification.

CYBERSECURITY RISK MANAGEMENT

A-25. Cybersecurity risk management identifies and analyzes threats against, and vulnerabilities of, networks and information systems; assesses the threat level; and determines how to deal with risks. Risk management also includes identifying vulnerabilities created by design weaknesses, ineffective security procedures, or faulty internal controls, which are susceptible to exploitation. See DODI 8510.01 for more information on cybersecurity risk management.

A-26. Risk management is a holistic activity integrated into every aspect of the organization. Figure A-2 on page A-9 illustrates the three tiers of cybersecurity risk management. This tiered approach addresses risk-related concerns at the organization, mission and business process, and information systems levels.

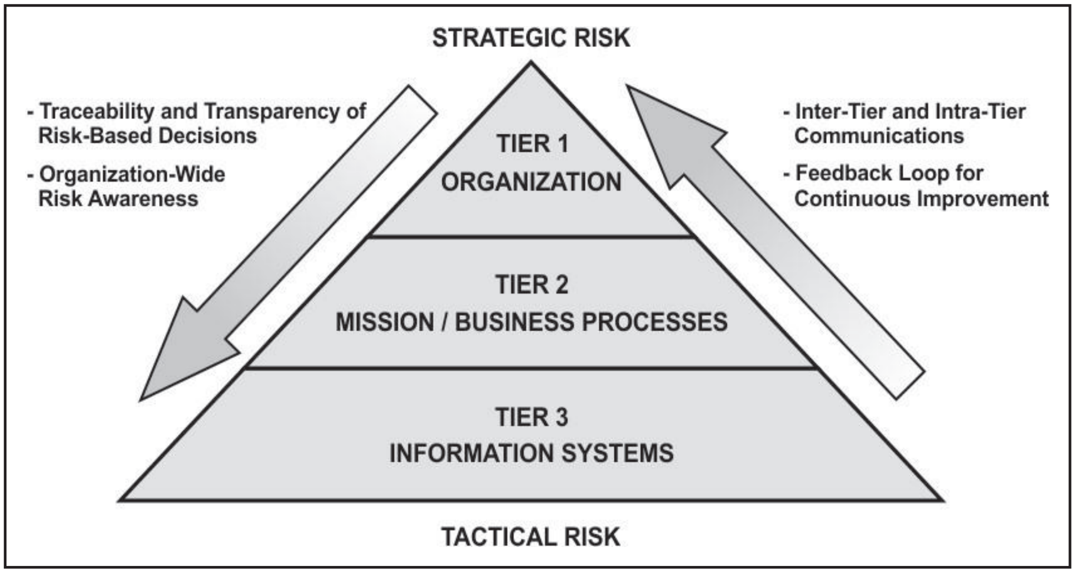

STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
TIER 1
ORGANIZATION
- Inter-Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
TACTICAL RISK

Figure A-2. Cybersecurity risk management

A-27. Risk management at tier 1 addresses organizational risk. Tier 2 and 3 risk decisions inform and influence tier 1 risk management as part of the feedback loop.

A-28. A comprehensive information systems security governance structure aligns information systems security strategies to support mission and business objectives, ensures they are consistent with applicable laws and regulations, and assigns responsibilities.

A-29. The DOD information security risk management committee is comprised of the four mission area principal authorizing officials and other major DOD and intelligence community stakeholders. The information security risk management committee provides tier 1 risk management governance for the DOD.

A-30. Tier 2 addresses mission and business process risks. Tier 1 risk decisions guide, and tier 3 risk decisions inform and influence, tier 2 risk management.

- The activities at tier 2 begin with designing, developing, and implementing the mission and business processes defined at tier 1.
- The principal authorizing officials for each DOD mission area provide tier 2 governance for their respective mission areas.

A-31. Tier 3 addresses information systems and platform IT system risk. Tier 1 and 2 risk decisions guide tier 3 risk management.

- Requirement identification for specific protective measures takes place at tiers 1 and 2. Tier 3 includes applying the protective measures identified at tiers 1 and 2.
- Selecting and implementing appropriate security controls from National Institute of Standards and Technology Special Publication 800-53 satisfies information protection requirements.

RISK MANAGEMENT FRAMEWORK

A-32. The risk management framework (formerly the DOD Information Assurance Certification and Accreditation Process) provides a disciplined and structured process for combining information systems security and risk management into the system development life cycle. The DOD risk management framework complies with National Institute of Standards and Technology guidelines to align with federal civilian agencies. The risk management framework has six steps—

- Categorize system.
  - Describe the system, including the system boundary, and document the description in the security plan.

  - Register the system with the DOD Component cybersecurity program.
  - Assign qualified personnel to risk management framework roles.
- Select security controls.
  - Identify common controls.
  - Identify the security control baseline for the system and document in the security plan.
  - Develop and document a system-level strategy for continuously monitoring the effectiveness of security controls and proposed or actual changes to the system and its operating environment.
  - Develop and implement processes whereby the authorizing official reviews and approves the security plan and system-level continuous monitoring strategy.
- Implement security controls specified in the security plan in accordance with DOD implementation guidance.
- Assess security controls.
  - Develop, review, and approve a plan to assess security controls using a methodology consistent with National Institute of Standards and Technology Special Publication 800-30.
  - Assess security controls in accordance with the security assessment plan and DOD assessment procedures.
  - Record the compliance status of security controls.
  - Assign vulnerability severity value for security controls.
  - Determine risk level for security controls.
  - Assess and characterize the aggregate level of risk to the system.
- Authorize system.
  - Prepare the program of action and milestones based on the vulnerabilities identified during the security control assessment.
  - Assemble the security authorization package and submit to the authorizing official for adjudication.
  - Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.
  - Decide whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable.
  - If the risk is determined to be unacceptable, issue a denial of authorization to operate. If the system is already operational, the authorizing official will issue a denial of authorization to operate and stop operation of the system immediately.
- Monitor security controls.
  - Determine the security impact of proposed or actual changes to the information system or platform IT system and its environment of operation.
  - Assess a subset of the security controls employed within and inherited by the information system or platform IT system in accordance with the system-level continuous monitoring strategy.
  - Conduct remediation actions based on the results of ongoing monitoring activities, risk assessment, and outstanding items in the program of action and milestones.
  - The program manager or system manager updates the security plan and program of action and milestones, based on the results of the system-level continuous monitoring process. The information system security manager may recommend changes or improvements to the implementation of assigned security controls, the assignment of additional security controls, or changes or improvements to the design of the system to the security control assessor and authorizing official.
  - Report the security status of the system, including the effectiveness of security controls, to the authorizing official and other appropriate organizational officials, in accordance with the monitoring strategy.

  - The authorizing official continues to review the reported security status of the system, including the effectiveness of security controls, in accordance with the monitoring strategy, to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable.
  - Implement a system decommissioning strategy, when needed. The decommissioning strategy defines the actions required when removing an information system or platform IT system from service.

A-33. **Cybersecurity reciprocity** aids rapid, efficient IT capability development and fielding. Reciprocity reduces redundant testing, assessment, and documentation, and the associated costs in time and resources. The risk management framework presumes acceptance of existing test and assessment results and authorization documentation from other Services and federal agencies.

A-34. The Services share security authorization packages and agree to accept other Services' test and assessment results and authorization to support cybersecurity reciprocity. Reciprocal acceptance of DOD and other federal agency and department security authorizations ensures interoperability and reduces redundant testing. It is important that each Service exercises due diligence in assessing, documenting, and approving systems, software, and configurations, since all Services share a risk accepted by one Service.

Note. See DODI 8510.01 for detailed, authoritative guidance on implementing the risk management framework.

OPERATIONAL RESILIENCE

A-35. DODIN operations personnel install, operate, maintain, and secure IT systems to—

- Ensure information and services are available to authorized users when and where they are required according to mission needs, priorities, and changing roles and responsibilities.
- Sense and correlate security posture, from individual devices or software objects to systems, and make it visible to mission owners and network operators across the DODIN.
- Ensure that whenever possible, hardware and software can reconfigure, optimize, self-defend, and recover with minimal human intervention. Attempts to reconfigure, self-defend, and recover should produce an incident audit trail.

A-36. Operational resilience requires three conditions be met:

- Information resources are trustworthy.
- Missions are ready for information resource degradation or loss.
- DODIN operations have the means to prevail in the face of adverse events.

A-37. Operational resilience is achieved by—

- Using trusted system and network requirements and best practices to protect mission-critical functions and components and manage risks.
- Performing developmental cybersecurity test and evaluation to inform acquisition and fielding decisions. This includes testing the ability of systems to detect and react to penetrations and exploitations and to protect and restore data and information.
- Including cybersecurity as a key element of program planning activities.
- Planning for mission continuation in the face of degraded or unavailable information resources.
- Conducting periodic exercises or evaluations of the ability to operate during loss of all information resources and connectivity.
- Preserving trust in the security of DOD information during transmission.
  - Protecting transmission of DOD information through established COMSEC and transmission security controls.
  - Conducting COMSEC monitoring and cybersecurity readiness testing.
- Applying compromising emanations (TEMPEST) countermeasures.

Cybersecurity Integration and Interoperability

A-38. Cybersecurity is integral to system life cycles. Adhering to the DOD IT architecture, a standards-based approach, and risk sharing among DOD Components helps achieve interoperability.

A-39. Cybersecurity personnel manage IT interconnections to reduce shared risk. Reducing vulnerabilities of each managed system protects the security posture of other interconnected systems.

Net-Centric Operations

A-40. A net-centric model provides personnel, services, and platforms the ability to discover one another and connect to form new capabilities or teams without being constrained by geographic, organizational, or technical barriers. The net-centric model allows collaboration to achieve shared ends. Cybersecurity design, organization, and management ensure systems can work together in any combination and maintain an expected level of readiness.

Integration

A-41. Cybersecurity is a visible element of organizational, joint, and DOD component architectures, capability identification and development processes, integrated testing, IT portfolios, acquisition, operational readiness assessments, supply chain risk management, security system engineering, and operations and maintenance.

Interoperability

A-42. Cybersecurity products—firewalls, file integrity checkers, virus scanners, intrusion detection systems, anti-malware—operate in a net-centric manner to enhance data exchange and shared security.

A-43. Semantic, technical, and policy interoperability integrate a wide range of cybersecurity products into a net-centric enterprise. This integration creates new information about the network and speeds up decision making and decision implementation.

A-44. Interoperability support products provide security for communications between different IT systems. The goal is seamless and secure exchange of critical classified or sensitive information.

Standards-Based Approach

A-45. One goal of the DOD cybersecurity strategy is interoperability through a standards-based approach. These standards conform to government, industry, and academic best business practices, and are available online from the National Institute of Standards and Technology Computer Security Resource Center.

Department of Defense Architecture Principles

A-46. Adhering to established DOD cybersecurity architectures enables interoperability and effective security management. All DOD Components use the same architectures to facilitate information sharing while managing the risk inherent in interconnecting systems.

Knowledge Repositories

A-47. Cybersecurity knowledge repositories enable sharing of best practices, benchmarks, standards, templates, checklists, tools, guidelines, rules, and principles. Examples include the National Vulnerability Database the Open Vulnerability and Assessment Language Repository and the Risk Management Framework Knowledge Service. Knowledge repositories enable policy and process interoperability and allow information sharing among cybersecurity professionals.

Cyberspace Defense

A-48. *Cyberspace defense* is actions normally created within Department of Defense cyberspace for securing, operating, and defending the Department of Defense information network. Specific actions include protect, detect, characterize, counter, and mitigate (DODI 8500.01).

A-49. Cyberspace defense protects against, detects, characterizes, counters, and mitigates unauthorized activity and vulnerabilities on the DODIN. Sharing cyberspace defense information across the enterprise supports shared situational understanding. Cyberspace defense actions create desired effects inside the DODIN and other specified cyberspace.

A-50. Cyberspace defense uses architectures, cybersecurity, intelligence, counterintelligence, other security programs, law enforcement, and other military capabilities to—

- Make the DODIN more resistant to penetration and disruption.
- Facilitate response to unauthorized activity.
- Defend information and networks against cyberspace risks.
- Recover quickly from cyber incidents.

Department of Defense Information Technology

A-51. USCYBERCOM controls access to and defense of DOD IT systems and information networks. Cyberspace defense integrates with other elements of DODIN operations to secure IT systems.

Continuous Monitoring Capability

A-52. Continuous network and information systems monitoring provide consistent collection, transmission, storage, aggregation, and presentation of current operational status to affected DOD stakeholders. A common monitoring framework, terminology, and workflow across DOD components ensure interoperability and shared situational understanding.

Penetration and Exploitation Testing

A-53. Penetration and exploitation testing are part of developmental and operational test and evaluation. This evaluation includes independent threat representative (cyber protection team or cyber red team) penetration and exploitation testing and evaluation of all cyberspace defenses. This testing includes the controls and protection provided by network defense service providers. For more information, see CJCSM 6510.03.

A-54. As part of the risk assessment process, cybersecurity professionals should periodically request penetration and exploitation testing. Testing measures the level of performance and effectiveness of cyberspace defense actions. For more information, see AR 380-53.

Law Enforcement and Counterintelligence

A-55. The DOD Cyber Crime Center provides digital and multimedia forensics and specialized cyberspace investigative training and services. The DOD Cyber Crime Center coordinates working relationships across the law enforcement, intelligence, and homeland security communities.

A-56. Individual Service law enforcement and counterintelligence agencies deploy their investigative capabilities on DOD networks to identify and investigate human threats to IT systems and information. Cybersecurity supports counterespionage, counterterrorism, and counterintelligence insider threat detection.

A-57. Network administrators accommodate lawful deployment of law enforcement and counterintelligence tools. DOD law enforcement and counterintelligence organizations coordinate law enforcement and counterintelligence efforts with their respective authorizing officials, consistent with service level agreements and change management processes. Coordination helps avoid disrupting mission-critical systems and networks.

Insider Threat

A-58. An *insider threat* is the threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities (CNSSI 4009). Trusted insiders with legitimate access to systems pose one of the most difficult threats to counter. Insiders are the most dangerous threat to operations security because they can readily access sensitive information. Whether recruited or self-motivated, insiders can access systems normally protected against attack, usually without raising suspicion. For this reason, operationally sensitive and critical information should only be shared with personnel who have both an appropriate security clearance and a valid need to know. While insiders can attack at almost any time, systems are most vulnerable during the design, production, transport, and maintenance stages. Risks from insiders may be intentional and malicious, or may cause damage unintentionally through negligence or inaction. Operations security awareness and learning to recognize threat indicators help identify and mitigate risks from insider threats. Reportable cyber indicators of a potential insider threat include—

- Excessive probing or scanning from either an internal or external source.
- Tampering with or introducing unauthorized data, software, or hardware into information systems.
- Hacking or password cracking activities.
- Unauthorized network access or unexplained user account.
- Social engineering, electronic elicitation, e-mail spoofing, or spear phishing.
- Use of DOD account credentials by unauthorized parties.
- Downloading, attempting to download, or installing non-approved computer applications.
- Key logging.
- Rootkits, remote access tools, and other backdoors.
- Unauthorized account privilege escalation.
- Account masquerading—changing credentials to look like another user's credentials.
- Unexplained storage of encrypted data.
- Encryption or steganography (hiding a coded message within an ordinary message) data propagation internally.
- Unauthorized use of USB removable media or other transfer devices.
- Denial of service attacks or suspicious network communication failures.
- Exfiltration of data to unauthorized domains or cross-domain violations.
- Unauthorized e-mail traffic to foreign destinations.
- Unauthorized downloads or uploads of sensitive data.
- Use of malicious code or blended threats such as viruses, worms, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration.
- Data or software deletion.
- Log manipulation.
- Unauthorized use of intrusion detection systems.

A-59. All personnel need annual threat awareness and reporting program training to maintain awareness of extremist, espionage, and insider threat indicators. See AR 381-12 for more information about the threat awareness and reporting program.

CYBERSECURITY PERFORMANCE

A-60. Cybersecurity personnel measure, assess, and manage systems' performance relative to their contributions to mission outcomes and strategic goals and objectives. They collect data to support reporting and cybersecurity management across the system life cycle. Standardized IT tools, methods, and processes prevent duplicate costs and focus resources on technologically mature and verified solutions.

A-61. Services implement processes and procedures to accommodate three conditions necessary for consistent cybersecurity across the DOD—

- Organization direction—organizational mechanisms for establishing and communicating priorities and objectives, principles, policies, standards, and performance measures.
- A culture of accountability—aligning internal processes; maintaining accountability; and informing, making, and following through on cyberspace protection and defense decisions.
- Insight and oversight—measuring, reviewing, verifying, monitoring, facilitating, and remediating to ensure coordinated and consistent cybersecurity compliance without impeding local missions.

Department of Defense Information

A-62. The DOD cybersecurity program provides the mechanisms to measure, monitor, and enforce information security and information sharing policies and procedures as they relate to information in an electronic form, primarily by implementing security controls.

A-63. Information security guidance establishes the standards for protecting classified and controlled unclassified information. Information systems protect classified and controlled unclassified information from unauthorized access by requiring user authentication.

A-64. A security domain is a system or network, such as NIPRNET, SIPRNET, or Joint Worldwide Intelligence Communications System, that operates at a particular sensitivity level. Transferring data between security domains, for example between NIPRNET and SIPRNET, requires a cross domain solution. A *cross domain solution* is a form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains (CNSSI 4009). Cross domain solutions need careful control because of the damage that can result due to spillage from a higher domain to a lower classification, for example secret information spilled onto NIPRNET.

A-65. A privacy impact assessment is required for DOD information systems that collect, maintain, use, or disseminate personally identifiable information about members of the public, federal personnel, contractors, or foreign nationals employed at U.S. military facilities (see DODD 5400.07).

Identity Assurance

A-66. Identity assurance ensures strong identification and authentication and eliminates anonymity in DOD information systems and platform IT systems. The DOD uses department-wide public key infrastructure and public key infrastructure-enabled information systems. Cybersecurity personnel manage and safeguard biometric data supporting identity assurance according to applicable DOD and Army policies.

A-67. DOD information systems use only DOD-approved identity credentials to authenticate entities requesting access to or within the DODIN. This requirement extends to mission partners using DOD information systems.

Information Technology

A-68. IT systems that receive, process, store, display, or transmit DOD information are acquired, configured, operated, maintained, and disposed of consistent with established cybersecurity policies, standards, and architectures. Planners identify cybersecurity requirements and consider them throughout the system life cycle.

A-69. Global sourcing and distribution and weaknesses or flaws in information technologies carry inherent risks. These vulnerabilities require careful management and monitoring to mitigate risks.

Cybersecurity Workforce

A-70. Security configuration errors make DOD networks and information systems vulnerable to attack or failure. For this reason, cybersecurity personnel require careful screening and appropriate technical qualifications, according to DODD 8140.01. Cybersecurity managers ensure cybersecurity personnel have the required certifications base on their roles and integrate them across the range of military operations.

Mission Partners

A-71. Standards-based cybersecurity enables seamless collaboration with mission partners. The decision structures and processes in DODI 8500.01 govern shared cybersecurity.

A-72. DOD information residing on mission partner information systems requires adequate safeguards. Documented inter-agency and multinational agreements specify the required levels of protection.

CYBERSECURITY SERVICES

A-73. Cybersecurity includes both technical and non-technical measures, such as risk management, personnel training, audits, and continuity of operations planning. Cybersecurity factors in all cyber incidents that occur through malicious or accidental activity by enemy, adversary or friendly entities.

A-74. *Critical infrastructure protection* is actions taken to prevent, remediate, or mitigate the man-made or natural risks to critical infrastructure and key assets (JP 3-28). Depending on the risk, these actions could include—

- Changing tactics, techniques, or procedures.
- Adding redundancy.
- Selecting another asset.
- Isolating or hardening affected systems.
- Guarding affected systems.

FUNCTIONAL SERVICES

A-75. The ten functional services of cybersecurity help protect friendly information, networks, and information systems while denying adversaries access to the same information, networks, and information systems. These functional services are—

- **Access control** provides the capability to restrict access to resources and protect them from unauthorized modification or disclosure. Access control measures can be technical, physical, or administrative. Access control uses hardware tools, software tools, or operational procedures.
- **Application security** protects software applications and software solution development. Some examples of application security solutions are software update service and patch management.
- **A continuity of operations plan** provides preservation and post-disaster recovery of information, network, or information system resources in case of incidents that interrupt or may interrupt normal operations.
- **COMSEC** provides the principles, means, and methods of encrypting voice, video, data, and imagery to ensure confidentiality, integrity, authentication, and nonrepudiation.
- **Risk analysis** identifies information assets, identifies risks, quantifies the possible damages that can occur to those information assets, and determines the most cost-effective way to mitigate the risks. Risk mitigation may include developing and implementing policies, standards, procedures, and guidelines.
- **Legal and regulatory compliance** fulfill the requirement for individuals to know and understand cybersecurity based on U.S. laws and DOD or Army regulations. Compliance also assists investigations to detect defensive breaches.
- **Development of cybersecurity policies and procedures** related to organizational personnel, hardware, software, and media. Cybersecurity policies and procedures identify security guidelines for data, media, telecommunications equipment, and information systems. These policies and procedures also help ensure the security of the users' activities. Examples of required activities are monitoring activity logs and analyzing audit trails.
- **Physical (environmental) security** protects the network facility from the outside perimeter to the inside operational space, including all information system resources. Physical security safeguards the network and information systems against damage, loss, and theft. Physical security includes determining and integrating site selection criteria and implementing effective perimeter and interior security for those facilities. Site selection also includes measures to enable adequate temperature, humidity, and fire controls.
- **Security in development and acquisition** implements principles, structures, and standards for hardware and software acquisition to enforce confidentiality, integrity, and availability. The key is integrating the common security criteria across DOD, Army, and international standards, including the trusted computing base and reference monitor models.
- **Telecommunications and network security** include implementing network architectures; transmission methods; transport formats; measures to provide confidentiality, integrity, and

availability; and authentication for transmission over private and public communications networks and media. Secure networks incorporate cross domain solutions, remote access protocols, IP security, virtual private networking, and access control lists. Some common solutions include intrusion detection and prevention systems, antivirus solutions, web caches, and firewalls.

CYBERSECURITY FUNCTIONS

A-76. Cybersecurity functions help an organization manage risk by organizing information, enabling risk management decisions, mitigating threats, and improving security by learning from earlier activities. These functions align with existing incident management methodologies and help show the impact of cybersecurity measures.

A-77. The cybersecurity functions are—

- Identify.
- Protect.
- Detect.
- Respond.
- Recover.

A-78. Cybersecurity personnel perform these functions concurrently and continuously to mitigate the dynamic cyberspace risk.

Identify

A-79. The identify function develops situational understanding to manage cybersecurity risks to systems, assets, data, and capabilities. This function helps cybersecurity personnel understand the mission, the resources supporting critical functions, and related cybersecurity risks. This understanding allows an organization to focus and prioritize its efforts, consistent with its risk management strategy and mission needs.

Identify Mission-Critical Assets

A-80. Mission-critical assets are those resources without which the unit's key missions would significantly degrade or cease to function. The steps in identifying mission-critical assets are—

- Inventory the organization's physical devices, systems, and software applications.
- Map the associated communication and data flows.
- Understand cybersecurity roles and responsibilities of higher and subordinate units.
- Identify the security categories for resources.

A-81. Information systems have assigned security categories, based on the potential impact of a breach to the security objectives of confidentiality, integrity, and availability. The security category (low, moderate, or high) determines the necessary cybersecurity controls.

A-82. Cybersecurity professionals and system owners identify mission-critical assets by determining the potential impact if there is a loss of—

- Confidentiality.
- Integrity.
- Availability.

A-83. Identifying mission-critical assets and their security categories is a continual process. The process is mission-dependent and synchronized with the military decision-making process. Mission-critical assets may change rapidly based on operational phases, outcomes of running estimates, refined commander's intent, commander's critical information requirements, and essential elements of friendly information. Refer to Federal Information Processing Standards Publication 199 for more information on security categorization.

Identify Laws, Regulations, and Policies

A-84. Cybersecurity professionals must understand and follow applicable Army, DOD, and national laws, policies, and processes to meet regulatory, legal, risk, environmental, and operational requirements. They also develop internal policies and procedures for their organizations to mitigate cybersecurity gaps or leader requirements the existing laws, policies, and processes do not cover.

Identify Threat Activities

A-85. Threat actors can exploit system vulnerabilities and cause a loss of confidentiality, integrity, or availability of communications networks. These threat actors use many methods to disrupt, degrade, destroy, exploit, alter, or otherwise adversely affect the Army's use of cyberspace. Threat agent categories, methodologies, and intents include—

- **Unauthorized users**, such as hackers, are the source of most attacks against information systems in peacetime. They mostly target personal computers but have also targeted network communications, mainframes, and local area network-based computers.
- **Trusted insiders** with legitimate access to systems pose one of the most difficult threats to counter. Whether recruited or self-motivated, insiders can access systems normally protected against attack without leaving any indicators of malicious or unusual activity.
- **Terrorist groups** with access to commercial information systems, including the Internet, may access an information network without authorization, or direct physical attacks against the infrastructure. Organized terrorist groups pose serious threats to the information infrastructure and U.S. national security.
- **Non-state groups**, such as drug cartels and social activists, can take advantage of the information age to acquire the capabilities to strike at their foes' commercial, security, and communications infrastructures at low cost. Moreover, they can strike from any distance with near impunity.
- **Foreign intelligence entities**, which are active during both peacetime and conflict, take advantage of the anonymity offered by computers, bulletin boards, and the Internet. They hide organized collection or disruption activities behind the facade of unorganized attackers. Their primary targets are often commercial, scientific, and university networks. Foreign intelligence entities may also directly attack military and government networks and systems.
- **Opposing militaries or political opponents** are more traditionally associated with open conflict or war, but these attackers may invade U.S. computer and telecommunications networks during peacetime. Such strikes may seek to help frame situations to their advantage preceding the onset of hostilities.

A-86. Risks to the DODIN and Army networks are natural or man-made, worldwide in origin, technically multifaceted, and growing. They may come from individuals or groups motivated by military, political, cultural, ethnic, religious, personal, or industrial gain.

A-87. To understand intentional, malicious cyberspace attacks, cybersecurity professionals request information on the latest threat tactics, techniques, and procedures from supporting intelligence elements. Cybersecurity professionals monitor external data sources, for example vendor sites and computer emergency response teams, to maintain awareness of threat conditions and identify which security issues may affect their network.

A-88. Adversaries use cyberspace attacks against the DODIN to deny, degrade, disrupt, destroy, manipulate, or otherwise adversely affect friendly forces' ability to use cyberspace. The DODIN consists of several segments spanning multiple domains, with many means of communicating and different levels of interconnectivity and isolation. For this reason, enemies may employ a wide spectrum of capabilities to conduct offensive operations in the Army's portion of cyberspace. These capabilities may target any part of the DODIN, from specific nodes and links to the data traversing those nodes and links.

A-89. Friendly use of cyberspace requires control of the physical, logical, and cyber persona layers and the electromagnetic spectrum. Threat cyberspace attacks may target any of these to deny friendly cyberspace use. The cyber persona layer is vulnerable to social engineering and phishing. The logical network layer may be subject to cyberspace attack. The physical network layer may experience a physical or lethal attack. An adversary may try to deny access to the electromagnetic spectrum through an electronic attack, such as jamming. Figure A-3 shows the cyberspace threat aspects.

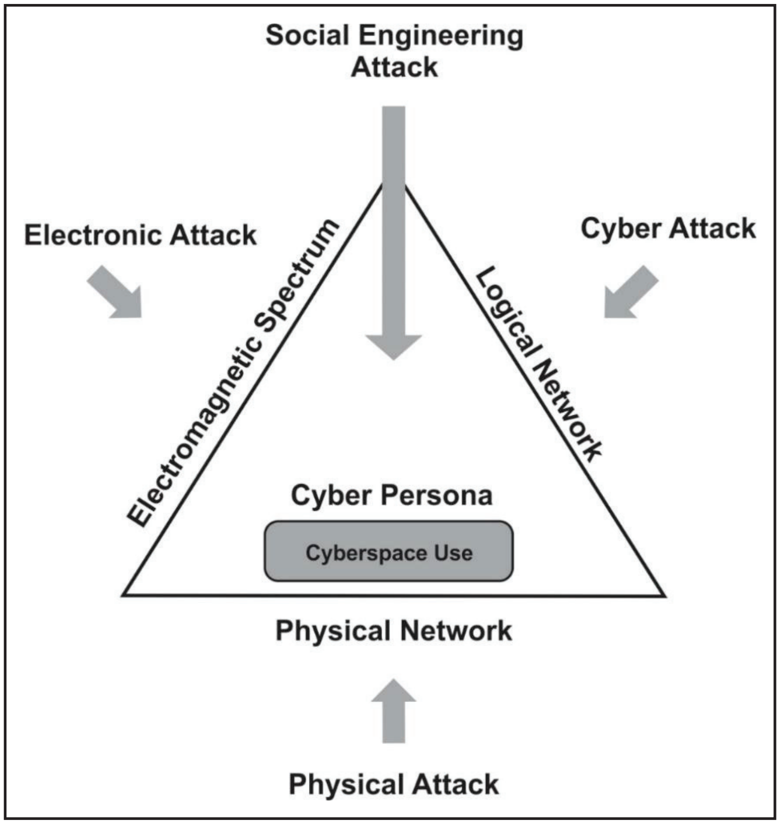


Figure A-3. Cyberspace threat aspects

- **Cyberspace attacks** are actions that create various direct denial effects in cyberspace (degradation, disruption, or destruction) or manipulation that leads to hidden denial, or that manifests in the air, land, maritime, or space domain.
- ***Electronic attack*** is the division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires (JP 3-13.1).
- **Physical attacks** use measures to physically destroy or otherwise adversely affect a target. Because cyberspace network enclaves can be isolated, this may involve lethal attacks on network nodes. A physical attack can create effects within and outside cyberspace to help control the domain. Regardless of the degree of isolation, an adversary may decide a direct physical attack is the best option depending on the situation, the desired effect, and availability and suitability of other capabilities or options.
- **Social engineering** describes a non-technical intrusion that relies on human interaction, Social engineering involves tricking others into divulging information or violating security procedures. For example, a person using social engineering to break into the DODIN might try to gain the confidence of an authorized user and get them to reveal information, such as a password, that compromises network security. Social engineers rely on the natural helpfulness of people, as well as their weaknesses. Virus writers use social engineering to persuade people to run malware-laden e-mail attachments. Phishers use social engineering to convince people to divulge sensitive information. Scam software vendors may use social engineering to frighten people into running software that is either useless or malicious.

A-90. The outcome of adversary cyberspace activities is either an incident or event:

- *Cyber Incident*—Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein (CNSSI 4009).
- *Event*—Any observable occurrence in a network or system (CNSSI 4009). Events sometimes indicate that a cyber incident is occurring.

A-91. Adversary cyberspace attacks can cause effects to communications, command and control capabilities, and other operational missions, such as fires. An adversary's ability to access cyberspace can result in a change to the information in Army systems. This change can influence future friendly actions or lead to reduced confidence in DOD information. This reduced confidence degrades situational understanding of the information environment. For more information on cyberspace threat, see FM 3-12.

Identify Vulnerabilities

A-92. Deploying forces require secure video, database connectivity, and the ability to send and receive data to enable reach operations, access to intelligence, and other essential support. Successful operations require reachback to access information residing outside the operational area. Soldiers' mobility and sustainment requirements may rely on commercial reach telecommunications, including international telecommunications and public switched networks.

A-93. Soldiers' increased reliance on reachback information capabilities creates vulnerabilities to attack from various sources. Adversaries can quickly exploit design weaknesses, ineffective or lax security, or insufficient internal controls to attack networks and information systems. Even an adversary who is not a technological equal could launch a covert or overt attack using inexpensive, commercial off-the-shelf products and readily available hacking tools. An adversary can attack from any location with Internet access. Recent trends that increase vulnerability include using commercial services, commercial off-the-shelf hardware and software; moving toward an open systems environment; and extensive interfacing with U.S. Government, industry, and public networks.

A-94. Vulnerabilities are flaws, loopholes, oversights, or errors a threat source can exploit. Vulnerability classification is based on the type of asset.

- Hardware and physical sites are vulnerable to environmental factors and uncontrolled access.
- Software is vulnerable to security flaws, software bugs, and poor password management.
- Insecure network architecture and complexity make networks vulnerable.
- Personnel are vulnerable due to inadequate security practices (visiting malicious websites).
- The lack of continuity plans, lack of audits, and failure to implement lessons learned make organizations vulnerable.

A-95. Vulnerability assessment includes systematically identifying and mitigating software, hardware, and procedural vulnerabilities. Auditing or penetration testing may identify some vulnerabilities. Assessment tools and techniques will search for and discover most vulnerabilities.

A-96. A major element of a vulnerability assessment is vulnerability scanning. Cybersecurity personnel conduct scheduled and unscheduled scans throughout all phases of operations. Operational scanning occurs in every layer of classified and unclassified networks. Both scheduled and no-notice scans are part of security policy and compliance enforcement.

A-97. For improved interoperability, preferred assessment tools express vulnerabilities in the common vulnerabilities and exposures naming convention and use the Open Vulnerability and Assessment Language. Cybersecurity professionals use one or more of these tools to discover as many vulnerabilities as possible:

- **Host Scanning tools** scan critical system files, active processes, file shares, and the configuration and patch level of a particular system. The results produced from this type of tool are usually very detailed because they run on the host system at the same permission level as the user conducting the scan. Although host-based tools provide very detailed results, it is important for cybersecurity professionals to manage the volume of data produced from these scans.
- **Network scanning tools** scan available network services for vulnerabilities through banner grabbing, port status, protocol compliance, service behavior, or exploitation.

- **Web application scanning tools** are a specialized form of network or host scanner that interrogates web servers or scans web source code for known vulnerabilities. These tools search for the presence of default accounts, directory traversal attacks, form validation errors, unsecure cgi-bin files, demonstration web pages, and other vulnerabilities.
- **Database application scanning tools** are specialized network scanners, which interrogate database servers for known vulnerabilities.
- **Vulnerability and patch management tools** incorporate many aspects of vulnerability management. These tools apply to vulnerabilities, policy compliance, patch management, configuration management, and reporting. These solutions make managing large, complex networks more efficient and reduce manpower requirements.

A-98. System administrators and network managers need the consent of the information system security officer and the G-6 or S-6, who consider operational or mission status and bandwidth constraints before scanning. Table A-1 details the actions undertaken when scanning.

Table A-1. Scanning guidelines and actions

Step	*Scanning Guidelines/Actions*
1	System administrator obtains and maintains training and certification on Army-approved cybersecurity scanning tools from the Army Cybersecurity Portal.
2	System administrator reviews Army best business practices at the Army Cybersecurity Portal.
3	System administrator scans network-attached devices with Army-approved products monthly, or after receipt of an information assurance vulnerability alert.
4	System administrator reviews scan reports, identifies devices to patch, and updates locally created database or spreadsheet for future reference on false positives.
5	ISSO and system administrator manually or electronically apply patch.
6	ISSO and system administrator rescan network to verify patches.
7	ISSO and system administrator maintain scan results locally and report them to the commander and cybersecurity personnel, NEC, and information management area component functional chief information officer, RCC, or ACOIC.
8	ISSO and system administrator update Army Cyber Vulnerability Tracking databases with compliance information.

Legend:

ACOIC	Army Cyber Operations and Integration Center
ISSO	information system security officer
NEC	network enterprise center
RCC	regional cyber center

A-99. Sharing vulnerability scan results freely among appropriate personnel throughout the organization helps eliminate similar vulnerabilities in other systems. Vulnerability analysis for custom software and applications may require specialized approaches. These may include vulnerability scanning tools for applications, source code reviews, or static analysis of source code. If analysis identifies and verifies unauthorized activity, cybersecurity personnel follow the established incident and vulnerability reporting procedures, as outlined in CJCSM 6510.01 and AR 25-2.

A-100. Another major element of vulnerability assessment is managing vulnerabilities. Vulnerability management is a comprehensive process for notifying Services, DOD agencies and field activities, and joint and combatant commands about vulnerability alerts, bulletins, technical advisories, and countermeasures. Vulnerability management requires combatant commands, Services, and DOD agencies and field activities to acknowledge receipt, and provides specific time limits for implementing countermeasures, depending on the criticality of the vulnerability (CJCSM 6510.01). For the Army, ARCYBER is the lead agent for implementing IAVM. ARCYBER issues alerts, bulletins, technical tips, and system administrator reports based on mandatory USCYBERCOM IA vulnerability alerts and Army-generated IAVM requirements using DOD Enterprise E-mail and other vulnerability management systems, including—

- Army Network Operations Reporting Tool.

- Microsoft SYSMAN.
- Assured Compliance Assessment Solution.
- Continuous Monitoring and Risk Scoring.

A-101. Cybersecurity personnel perform routine vulnerability assessments and IAVM procedures to manage system and network vulnerabilities and maintain their remediation skills. DODIN operations personnel apply remediation actions specified in IAVM messages immediately. If they cannot implement an IAVM action, they must submit a mitigation plan in the Army Cyber Vulnerability Tracking databases for approval or disapproval.

Protect Function

A-102. Cybersecurity professionals, DODIN operations personnel, and users work together to develop and implement the appropriate safeguards to assure critical infrastructure services. The protect function supports the ability to limit or contain the impact of cybersecurity events. Each of the cyberspace layers (physical, logical, and cyber persona) and the electromagnetic spectrum have specific protection requirements. Figure A-4 depicts the cyberspace threat aspects from figure A-3 on page A-19 with the associated types of protection applied to mitigate each type of attack.

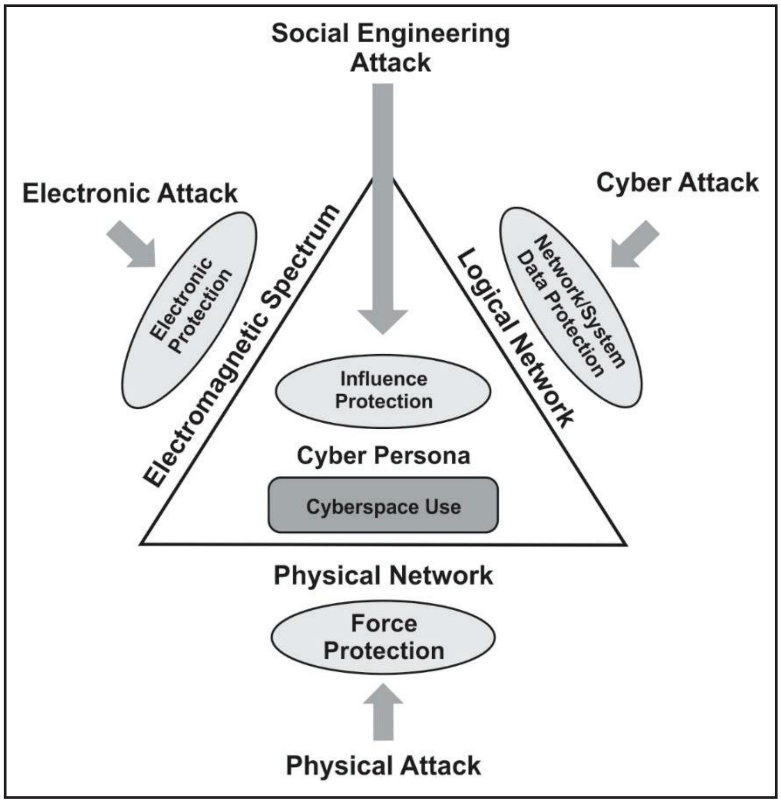


Figure A-4. Protection categories applied to cyberspace threat aspects

Information Operations Condition

A-103. The information operations condition (INFOCON) system establishes a uniform process for posturing and defending against malicious activity that targets DOD information systems and networks (Strategic Instruction 527-1). The DOD identifies the threat level against its networks and information systems by using INFOCON status levels. The INFOCON system provides coordinated, structured defense against, and reaction to, attacks on DOD computers, networks, and information systems. The INFOCON system outlines countermeasures to scanning, probing, unauthorized access, data browsing and general threats at DOD computers, networks, and information systems. Refer to Strategic Instruction 527-1 for more information on the INFOCON system.

Protect Networks, Systems, and Data

A-104. Protection of networks, information systems, and data is achieved using—

- **Identity and access control** ensures strong identification and authorization and eliminates anonymity in the network. Identity and access control restricts access to resources and protects them from unauthorized modification or disclosure. Access control measures may be technical, physical, or administrative (hardware or software tools or procedures). Within the DODIN-A, Army forces use public key infrastructure. DOD-approved identity credentials (common access card or SIPRNET hardware token) authenticate users. This requirement extends to mission partners using Army systems. Cybersecurity personnel manage authorized devices and user identities and determine whether to apply permissions based on information and knowledge management plans. Cybersecurity personnel also manage and protect remote access points.
- **COMSEC** provides the principles, means, and methods of encrypting voice, video, data, and imagery to ensure confidentiality, integrity, authentication, and non-repudiation. Cybersecurity professionals and network or system administrators ensure users employ COMSEC appropriately to protect data at rest and in transit.
- **Security in development and acquisition** implements principles, structures, and standards for hardware and software acquisition and life cycle management to enforce confidentiality, integrity, and availability. Cybersecurity personnel formally manage assets throughout procurement, implementation, transfer, removal, and disposition. Integrity checking mechanisms verify software and firmware in commercial products do not include malicious code.
- **Telecommunications and network security** includes implementing network architectures; transmission methods; transport formats; measures to provide confidentiality, integrity, and availability; and authentication for transmission over private and public communications networks and media. Secure networks incorporate cross domain solutions, firewalls, intrusion prevention and protection systems, web caches, IP security, virtual private networking, and access control lists. As part of telecommunications and network security, cybersecurity professionals verify the network's engineering ensures integrity and provides the network capacity needed to ensure availability.
- **Continuity of operations plans** preserve, and provide post-disaster recovery of, information, networks, or information system resources in case of incidents that interrupt or may interrupt normal operations.

Force Protection

A-105. Physical and environmental security measures support force protection. Environmental security protects the network facility from the outside perimeter to the inside operational space, including all information system resources. Physical security safeguards the network and information systems against damage, loss, and theft. Physical security planning includes determining and integrating site selection criteria and implementing effective perimeter and interior security. Site selection also includes measures to control environmental factors (temperature, humidity, and fire controls).

Electronic protection

A-106. *Electronic protection* is the division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability (JP 3-13.1). Electronic protection involves activities to address system hardening, electromagnetic compatibility, electromagnetic interference, reprogramming spectrum dependent devices, and emission control. Electronic protection focuses on both lethal and non-lethal electronic warfare activities. Electronic protection actions related to cybersecurity focus mainly on non-lethal electronic warfare. Electronic protection requires coordinating and integrating actions with electronic warfare and spectrum management personnel.

Influence Protection

A-107. The first line of defense against social engineering is the user. Cybersecurity professionals should develop internal standard operating procedures for managing potential social engineering attacks. They should ensure users complete periodic cybersecurity awareness training. Cybersecurity awareness training prepares users to perform information security-related duties consistent with applicable policies, procedures, and agreements.

A-108. Through social engineering attacks, adversaries seek out exploitable information to influence others. For this reason, operations security measures help achieve cybersecurity objectives. *Operations security* is a capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities (JP 3-13.3). Operations security helps prevent adversaries gaining critical information through cyberspace. Critical information includes indicators that are sensitive, but unclassified, such as passwords. Operations security aims to identify unclassified activity or information that, when analyzed with other activities and information, can reveal protected and important friendly operations, information, or activities. Cybersecurity professionals integrate their activities with operations security efforts to enhance the effectiveness of both.

Detect Function

A-109. Detection involves activities such as anomaly and event handling and continuous monitoring. Detection uses intrusion detection systems and other sensor and logging devices to discover and report anomalies. Intrusion detection systems require continuous monitoring to provide timely warning of incidents and attacks. Monitoring also requires both automated and manual analysis. When a potential attack is detected, tracing and monitoring determine the severity and extent of the attack, gather evidence, limit the attack's effects, identify the potential for escalation, coordinate responses, and determine the effectiveness of countermeasures.

A-110. Cybersecurity professionals maintain and test detection processes and procedures to ensure prompt, adequate identification of anomalies. Well-defined individual and facility detection roles and responsibilities ensure accountability. Moreover, detection activities follow approved concepts, methodologies, and best practices. The goal is continually improving the organization's detection processes.

Continuous Monitoring

A-111. NOSCs monitor networks and systems in near real-time to detect anomalies and take preliminary defensive actions. Continuous network and information systems monitoring identifies unauthorized network connections, devices, and software, using both automated and manual processes. Monitoring includes not only the network, but also the physical environment and personnel activities.

Anomalies and Events

A-112. The ability to detect an event depends on established baseline network and information system configurations and behaviors. The baseline serves a basis for comparison to discover and analyze changes to identify their cause and potential impact. Once cybersecurity personnel discover an incident and it reaches alert thresholds, they categorize and report it to the commander and higher-level DODIN operations authorities. Reporting allows DODIN operations personnel to aggregate and correlate events with other activities occurring in the cyberspace and physical domains.

A-113. Certain anomalies and events may require notifying law enforcement or counterintelligence agencies. Law enforcement and counterintelligence agencies can deploy capabilities on Army networks to identify and investigate the human element posing a threat to Army IT and DOD information. Cybersecurity personnel may support counterespionage, counterterrorism, and counterintelligence insider threat mitigation according to DODI 5240.26. Network administrators accommodate legitimate deployment of law enforcement and counterintelligence tools. Law enforcement and counterintelligence organizations, in turn, make all reasonable attempts to employ their solutions consistent with established change control processes to avoid disrupting mission-critical systems.

Respond Function

A-114. Response involves steps to limit and mitigate the effects of unauthorized network activity. Effective response requires well-defined processes and procedures for handling incidents in an organized and disciplined manner, including coordination with internal and external stakeholders, such as law enforcement and counterintelligence. Damage containment and control prevents the spread of malicious code, minimizes the effects of an attack, and reduces exposure of interconnected networks and systems. The response preserves evidence and remnant files to enable forensic analysis. Technical support, including the analysis of logs and related activities, aids in incident response.

Mitigation

A-115. Cybersecurity professionals work with network operators, leaders, and users to counter potential threats by recommending and implementing activities to prevent an event's spread, minimize its effects, and create conditions that allow its elimination from the network. This may involve changing network configurations, creating new policies, or adopting new tactics, techniques, and procedures.

Analysis

A-116. Once cybersecurity personnel mitigate an event to a level that allows for mission assurance, they collect relevant information logs for forensic analysis. Forensic analysis validates the incident type, the intrusion method used, and the impacted system's shortcomings. This analysis helps cybersecurity professionals understand the incident's technical details, root cause, and operational impact. This understanding helps determine other information to gather, coordinate information sharing with others, and develop a course of action for response. Cybersecurity professionals report incidents to higher-level DODIN operations authorities, law enforcement, and counterintelligence, describing the threat event in detail. These authorities correlate this information with other incidents across the DODIN to identify relationships and trends between incidents in the short term and patterns across threat activities in the long term.

Recover Function

A-117. Recovery reestablishes normal operation of the network. The recover function includes activities to remove the vulnerability from the network and information systems.

A-118. Recovery activities strive to improve operational, technical, and management controls to prevent recurrence of threat activity. After DODIN operations personnel follow the detailed recovery steps, cybersecurity professionals conduct a post-incident analysis to review the effectiveness of incident handling. Lessons learned from this analysis help in developing follow-up strategies that support prevention goals.

Cybersecurity Principles

A-119. The principles of cybersecurity are not a checklist and may not apply the same way in every situation. These principles offer cybersecurity professionals a context for implementing the cybersecurity framework, developing strategies, and allocating resources.

- **Full Dimension:** Cybersecurity is not a linear activity, but a continuous process. Cybersecurity efforts and activities account for cyberspace risks in all directions, in all environments, at all times. Cybersecurity planning, coordination, and implementation occur anywhere the protection against, detection of, response to, and recovery from anomalous network activity is required. Network situational understanding supports, and leads to proper implementation of, full dimension cybersecurity.
- **Layered:** Layered cybersecurity capabilities provide defense-in-depth. Layering reduces the destructive effects of a cyberspace attack. Layering may also provide time to focus response efforts.
- **Redundant:** Redundancy ensures critical activities, systems, efforts, and capabilities have secondary or auxiliary efforts of equal or greater capability. Redundancy in this context is not simple duplication of effort. It emphasizes overlapping capabilities for seamless protection. Cybersecurity professionals identify critical points of failure or critical paths for each

cybersecurity function, system, effort, and capability to apply redundancy. Cybersecurity efforts often overlap where there is an identified or expected vulnerability, weakness, or failure.

- **Integrated:** Cybersecurity integrates with all other cyberspace operations, systems, efforts, and capabilities. This adds strength and structure to the overall cybersecurity effort. Integration occurs throughout the DODIN operations hierarchy in all operations. Cybersecurity integration supports and complements other cyberspace operations.
- **Enduring:** Cybersecurity's enduring nature differentiates it from defensive cyberspace operations. Defensive cyberspace operations continue only until cyberspace forces can resume normal operation of the network, performing security to maintain freedom of action. Cybersecurity's persistent character preserves critical assets to enable mission assurance. Enduring cybersecurity affects freedom of action and resource allocation.

ENABLED EFFECTS

A-120. Cybersecurity enables information protection, and network and system availability. DODIN operations personnel achieve these by—

- Instituting agile capabilities, such as firewalls, password protection, intrusion detection, and intrusion prevention, to resist adversary attacks by recognizing such attacks as they begin or progress.
- Detecting and analyzing anomalies or intrusions and reporting incidents to all NOSCs and ARCYBER.
- Implementing efficient, effective responses to reduce the effects of an attack, and to recover from attacks safely and securely.
- Informing others across the DODIN of local actions to counter intrusions or correct other incidents.
- Certifying, accrediting, and reporting on all networks, peripherals, and edge devices in their portion of the network, and enforcing information security controls.
- Evaluating subordinate units' security readiness and vulnerability for compliance with communications tasking orders and IAVM, and reporting compliance to higher echelons.
- Ensuring network management and defense training, awareness, and certification program compliance according to established policies and directives.
- Developing and deconflicting local contingency plans to defend against malicious activity and providing copies to higher-level commands and DODIN operations authorities.
- Conducting network risk assessments.
- Sharing cybersecurity information according to formal agreements and national disclosure policies, except where limited by law, policy, or security classification.
- Submitting reports, as directed by higher commands and DODIN operations authorities.
- Developing and maintaining remediation, mitigation, and reconstitution plans for critical infrastructure protection criteria.
- Reconstituting capabilities from reserve or reallocated assets when original capabilities are destroyed.
- Coordinating between user elements to distinguish between hostile cyber incidents and other system outages or degradations.

MITIGATING INSIDER THREATS

A-121. The insider is anyone with current or past authorized access to a DOD information system. Potential insider threats include military members, DOD civilians, employees of other federal agencies, and contractors.

A-122. The insider threat is real and significant. A DOD Inspector General investigation determined 87 percent of identified intruders into DOD information systems were either employees or others internal to the organization. Insiders may cause security risks through—

- Malicious intent.

- Disdain for security practices.
- Carelessness.
- Ignorance of security policy, security practices, and proper information system use.

A-123. An effective insider threat mitigation strategy implements best practices across multiple disciplines. Key elements of this strategy include—

- Determine which assets are critical to the mission.
- Establish trustworthiness—seek to reduce the threat by establishing a high level of assurance in the trustworthiness of people, practices, systems, and programs thorough personnel security, cybersecurity awareness training, and cybersecurity best practices.
- Strengthen and enforce personnel security and management practices.
- Protect information assets by—
  - Controlling asset-sharing through cybersecurity.
  - Isolating information and capabilities, based on security clearance and need-to-know, through compartmentalization and system architecture.
  - Identifying and reducing known vulnerabilities through cybersecurity.
  - Employing and enforcing effective physical security policies.
- Detect problems through cybersecurity.
- React or respond to cyber incidents and events.
- Maintain command emphasis on the Army counterintelligence Threat Awareness and Reporting Program.

ATTACKS

A-124. Some attacks have delayed effects while others are immediate. Both delayed and immediate attacks may corrupt databases and control programs and may degrade or physically destroy the system attacked. Prompt attack detection is essential to initiating intrusion response and network restoration.

A-125. Computer attacks generally target software or data in either end-user computers or platform information technology systems. *Platform information technology* is information technology, both hardware and software, that is physically part of, dedicated to, or essential in real-time to the mission performance of special purpose systems (DODI 8500.01). Adversaries may attempt to unobtrusively access information, modify software and data, or destroy software and data. These activities may target one or more computers connected to a local area network or WAN. Computer attacks may occur during routine operations and may disrupt major military missions. These attacks can happen during both wartime and peacetime. Attacks can be part of a major nation-state attempt to cripple U.S. information infrastructure or come from mischievous or vengeful insiders, criminals, political dissidents, terrorists, or foreign intelligence entities.

A-126. Attackers may design attacks to unleash computer viruses, trigger future attacks, or install software that compromises or damages information and information systems. Malicious attacks may also involve unauthorized file exfiltration or deletion, or malicious software or data introduction. Malicious software is executable software code secretly introduced into a computer, including viruses, Trojan horses, and worms. Malicious data insertion, also known as spoofing, seeks to mislead users or disrupt systems operation. For example, an attack may disrupt a packet data network by introducing false routing table data into one or more routers. An attacker who denies service, or corrupts data on a wide scale may weaken user confidence in the information on the network by corrupting or sending false data.

A-127. Physical attacks generally deny service and involve destruction, damage, overrun, or capture of system components. These components may include end-user computers, communications devices, and network infrastructure components. Another form of physical attack is theft of cryptographic keys or passwords. This is a major concern, since these items can support subsequent electronic or computer attack or analysis activities.

A-128. Electronic attacks may focus on specific or multiple targets across a wide area. Attacks against communications links include jamming and signals intelligence exploitation. Jamming overwhelms friendly signals, corrupts data being transmitted, and may cause denial of service. Two types of signals intelligence operations are signal interception and analysis to compromise data and emitter direction findings; and geo-location to support signal analysis and physical attacks.

INFORMATION SYSTEMS SECURITY

A-129. Army cybersecurity programs include the full range of security measures. Information systems security succeeds only when all assets connected to the local area network and throughout the WAN adhere to common technical standards. Protection from intrusions into, or via, a WAN begins with coordinating information systems security between all of the Services and the Defense Information Systems Agency. All measures to detect, respond to, and report attacks and intrusions must adhere to public laws, applicable DOD directives, and Army regulations. All users, system administrators and DODIN operations managers require cybersecurity awareness and certification training. Training prepares users to reduce vulnerabilities and risks by taking proper actions, depending on their DODIN operations role.

PROTECTION LEVELS

A-130. Protection levels apply only to confidentiality requirements. Protection levels are based on the required clearance, formal access approval, and need-to-know of direct and indirect users who receive information from information systems without manual intervention and reliable human review. Protection levels indicate the level of trust placed in the system's technical capabilities. Service providers and users cooperate to implement the required protection level. Soldiers need assurance that their information systems have the level of protection or trust needed for mission success.

PROTECTION, DETECTION, AND REACTION CAPABILITIES

A-131. Information systems and networks are critical to the military's ability to conduct operations. Adequately securing networks and information systems against attack requires the ability to—

- Protect the information computer systems and data networks pass and store.
- Detect intrusions into the network or information systems as they happen.
- React to limit or reduce damage, and repair the network or information system.

Protection

A-132. Information protection consists of active and passive measures to secure and defend friendly information and information systems to ensure timely, accurate, and relevant friendly information. Information protection denies enemies, adversaries, and threat actors the opportunity to exploit friendly information and information systems for their own purposes. Information protection includes cybersecurity and electronic protection.

A-133. Information protection applies to any data medium or form, including hardcopy, electronic, magnetic, video, imagery, voice, telegraph, computer, and human. Information protection involves determining appropriate security measures, based on the value of information protected. Protection measures reflect the changing value of the information about each operational phase of the mission. Leaders, information producers, processors, and users ensure information protection.

A-134. Continuity of operations plans, operation plans, and operation orders specify the priorities for protecting networks and information systems. Protection measures consist of the firewalls, intrusion protection systems, and software that harden these systems against intruders. Protecting information stored on U.S. computers and flowing through the networks is vital.

A-135. Army network and system managers devise and implement comprehensive plans for a full range of security measures. These plans include external and internal perimeter protection. External perimeter protection consists of COMSEC, router filtering, access control lists, security guards, and physical isolation as barriers to outside networks, such as the Internet. Internal perimeter protection consists of firewalls and router filtering. These serve as barriers between echelons of interconnected networks and information systems. Internal COMSEC barriers are also required. Local workstation protection consists of individual access controls, configuration audit capability, protection and intrusion detection tools, and security procedures.

A-136. Protection against intrusions into friendly computer networks denies unauthorized entry and access and protects networks and systems. Operations security procedures allow commanders to identify actions that adversary intelligence systems and intruders observe and provides awareness of the indicators adversary intelligence systems might collect. Operations security identifies and selects information adversaries could exploit, and countermeasures to mitigate threats. Since most vulnerabilities result from human error, operations security training helps protect against network intrusions. Many measures affect operations security, including information security, transmission security, COMSEC, and emission control.

A-137. Commercial capabilities, such as imaging, positioning, and cellular systems, allow adversaries to access significant information about U.S. forces. The ability of Army and other Service personnel to send information directly from the battlefield via e-mail to points around the world presents an attractive target for potential adversary exploitation. These e-mails may contain sensitive or classified information. Improper disclosure of this information could endanger friendly personnel and compromise missions.

A-138. Information on Army web pages is also a security concern. Operations security guidelines for web pages are the same as for any other information within the Army. Sensitive and classified information requires protection against disclosure to unauthorized personnel.

A-139. Security measures actively and passively preserve the confidentiality, integrity, availability, and functionality of information systems. Protection includes real- and near real-time measures to prevent intrusions and restore affected devices or systems. These security measures include—

- Vigorous cybersecurity protection programs.
- Denial of unauthorized access.
- Hardening of programs and gateways using software and hardware tools.
- Quality assurance procedures in all program and hardware acquisition.
- Strict access controls for networked computers and other devices.

A-140. Transmission security secures information across the various networks. Trunk encryption devices, in-line encryption devices, frequency hopping, and time division multiplexing and modulation techniques usually secure transmissions. Transmission security helps ensure information security. Any nonsecure system or device connected or entering into a secure network must use in-line encryption between the network entry point and the entering equipment.

A-141. COMSEC protects information on networks and system devices. Keying variables enable encryption of voice and data passing through transmission devices and computers. The National Security Agency controls most encryption keys and governs local key generation, distribution, and storage.

A-142. *Information security* is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (CNSSI 4009). Information security policies deny unauthorized access to classified or sensitive information. These policies establish measures to prevent disclosure of valuable information from other aspects of communications, such as traffic flow or message analysis, and to enhance the authentication of communications.

Detection

A-143. Routine DODIN operations activities include security management and intrusion detection to detect violations of security policies. Selected events or occurrences, such as several failed login attempts in a defined period, are monitored using conventional protection and detection tools and devices. When DODIN operations managers detect violations, they act to prevent further violations and report the event to the commander, information system security officer, and next higher NOSC in the DODIN operations technical channels.

A-144. NOSCs monitor networks and systems in near real-time to detect anomalies and take preliminary defensive actions. Prompt defensive actions mitigate the damage and reduce the operational impact of insecurities.

Reaction

A-145. Reaction to a network or information system intrusion includes restoring essential information services. A detailed continuity of operations plan includes procedures for various levels of restoration and addresses various potential disasters. Immediate restoration may rely on backup or redundant network links or system components, backup databases, or alternate means of network transport.

A-146. DODIN operations managers do not need permission to react to attacks or intrusions if their activities conform to appropriate regulations, statutes, and public law. DODIN operations managers or system administrators take these emergency steps when they verify an intrusion—

- Stop the breach, if possible, and restore any destroyed or compromised data from backups or other identified continuity of operations capabilities.
- Follow cyber incident policy, as outlined in the standard operating procedure and applicable regulations.
- Report the incident to the commander, cybersecurity manager, or information system security officer.
- Report the incident to next higher level NOSC.

A-147. Security management devices and IAVM messages warn DODIN operations personnel of intrusion attempts, attacks, and other network and systems anomalies. The appropriate response to these alerts depends on the severity of the attack, intrusion, or breach. These alerts trigger appropriate response measures. DODIN operations managers need to consider operational or mission status before responding to alerts. Protecting information systems requires real-time security management as a component of DODIN operations. When detection occurs, DODIN operations managers may need to take one or more of these actions—

- Change boundaries and perimeters.
- Reconfigure firewalls, guards, and routers.
- Reroute traffic.
- Change encryption levels or re-key COMSEC devices.
- Zeroize suspected compromised communications.
- Re-establish a network without compromised members.
- Change passwords and authentication.

A-148. Response begins immediately upon anomaly detection. The objective of a response is to restore services to a level that supports acceptable, if reduced, operations. Restoration returns services to the same level as before to the event. Responses may be offensive or defensive. Defensive responses include all measures and countermeasures available to a commander to limit an adversary's attack, exploitation, military deception, or electronic protection capabilities to protect against further attacks. See FM 3-12 for more information on defensive cyberspace operations-response actions.

INFORMATION ASSURANCE VULNERABILITY MANAGEMENT

A-149. *Information assurance vulnerability management* is the comprehensive distribution process for notifying combatant commands, Services, agencies and field activities about vulnerability alerts, bulletins, technical advisories, and countermeasures information. The IAVM program requires combatant commands, Services, agencies, and field activities to receipt acknowledgment and provides specific time parameters for implementing appropriate countermeasures depending on the criticality of the vulnerability (CJCSM 6510.01).

A-150. The IAVM program helps mitigate vulnerabilities. The ACOIC is the Army's lead agent for implementing IAVM. The Army Knowledge Online Knowledge Management Center mail service issues alerts, bulletins, technical tips, and system administrator reports for the ACOIC, based on mandatory ACOIC IA vulnerability alerts and Army-generated IAVM requirements.

A-151. IAVM is the program to identify and resolve discovered vulnerabilities on DOD systems and platforms. This program includes IA vulnerability alerts, IAVM messages, and technical advisories. IAVM requires completing four distinct phases to ensure compliance—

- Identifying, disseminating, and acknowledging vulnerabilities.

- Applying corrective measures to make affected systems compliant.
- Verifying compliance.
- Reporting compliance.

A-152. A patch is an immediate solution provided to users after the discovery of a vulnerability. Patches are often available from the software vendor's website.

A-153. Disseminating IA technical advisories, IAVM messages, and IA vulnerability alerts is automatic on registration completion. Cybersecurity personnel test system patches and fixes for interoperability and cybersecurity compliance before applying them.

A-154. DODIN operations personnel apply remediation actions specified in IAVM messages immediately. If they cannot implement an IAVM action, they must submit a mitigation plan in the Army Cyber Vulnerability Tracking databases for approval or disapproval.

Scanning and Remediation

A-155. Scanning is automated or semi-automated polling for information system and device configuration data. Scans help in system identification; maintenance; security assessment and investigation; verification of vulnerability compliance; or discovery of compromised systems. Scanning includes network port scanning and vulnerability scanning, whether wired or wireless, and classified or unclassified. Cybersecurity personnel conduct scheduled and unscheduled scans throughout all phases of operations.

A-156. Operational scanning occurs in every layer of the enterprise management structure and on all classifications of networks. Both scheduled and no-notice scans are part of security policy and compliance enforcement. NETCOM maintains scanning tool software licenses.

A-157. New vulnerabilities require proactive management. Assessors use a five-step methodology for assessment scanning—

- Identify assets.
- Determine vulnerabilities.
- Review vulnerabilities.
- Remediate vulnerabilities.
- Validate remediation measures.

A-158. The system administrator or network manager ensures confidentiality of information by preventing unauthorized access to computer equipment. The system administrator, network manager, and operators patch security vulnerabilities on all Army platforms. The NEC and tactical system administrators validate patches, whether the system is operating on the installation network or stored. Operation orders and other command directives should include these requirements.

A-159. System administrators reduce their systems' vulnerability by applying remediation actions including both hot fixes and service packs. Table A-2 on page A-32 details remediation actions.

Table A-2. Remediation actions

Step	*Remediation Actions*
1	Implement unit policy directing users to log off their workstations daily, but leave workstations on for patching during non-duty hours. The unit's cybersecurity manager identifies the day to apply patches.
2	Receive IAVM message identifying required patch.
3	Select required patches from the applicable website.
4	Ensure individual responsible for IAVM has administrative rights to the assets to scan and patch.
5	Scan devices (servers, routers, switches, and workstations) to identify those that require patching.
6	Identify test machine, apply patch, and scan to confirm patch application.
7	Apply patch to remaining devices.
8	Rescan to validate patch application.
9	Issue a conformance report (via patch application software).
Legend: IAVM information assurance vulnerability management	

CONTINUITY OF OPERATIONS

A-160. A continuity of operations plan is a plan for emergency response, backup operations, transfer of operations, and post-disaster recovery maintained by an activity as a part of its cybersecurity program. A continuity of operations plan ensures the organization can continue to function after a catastrophic event and defines procedures to protect and restore the organization's vital data and resume operations. Units conduct continuity of operations exercises at least annually. See AR 500-3 and DA Pam 25-1-2 for more detailed information on continuity of operations. Objectives of a continuity of operations plan include—

- Defining the organization's essential systems.
- Describing the personnel necessary to maintain systems.
- Defining the recovery objectives.
- Providing guidance for appropriate locations, timing, and actions to restore operations in an emergency.

DEPARTMENT OF DEFENSE INFORMATION NETWORK CONTENT MANAGEMENT

A-161. Managing and protecting networks and information systems for users does not ensure Soldiers receive relevant information to gain and maintain information advantage. Content management, comprised of information dissemination management and content staging, is the DODIN operations component that manages access to, and delivery of, relevant, accurate information to the appropriate users promptly, efficiently, and in the proper format.

A-162. Content management allows DODIN operations 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 relative to the information producers, information consumers, and mission requirements. Placing the content on servers closer to the end users reduces demands on limited network transport bandwidth. Content management objectives include—

- Enabling commanders to adjust information delivery methods and priorities for enhanced situational understanding.
- Enabling information producers to advertise, publish, and distribute information.
- Allowing users to define and set information needs to facilitate prompt, efficient information delivery.
- Allowing users to search information databases to retrieve desired products as they need them.

- Improving bandwidth utilization.
- Enhancing network transport capabilities by storing data as close as possible to the point of use to reduce bandwidth requirements.

A-163. Information dissemination management seeks to achieve the right information arriving at the right place and time, in a usable format. Information dissemination management uses specific processes, services, and applications to deliver this information. It provides awareness of—

- Relevant, accurate information.
- Automated access to new or recurring information.
- Prompt, efficient information delivery, based on commanders' priorities.

A-164. Information dissemination management efficiently delivers video, voice, and data products to commanders and their staffs, and ensures they know it is available. It uses a distribution system to integrate delivery and user notification. Information dissemination management allows users to—

- Define the types of information they need and have it delivered.
- Define information products they need and deliver them as requested.
- Access data from a variety of information systems.
- Retrieve relevant, accurate information to develop and maintain situational understanding.

A-165. Information dissemination management and content staging are enterprise-wide services used across the DOD to ensure information is available to all authorized users. Content management provides three core services—

- **Content discovery** provides the ability to quickly search for information throughout the DODIN. Users can search for data from multiple sources from one place, using any appropriate web browser on a desktop computer or wireless device, rather than making several separate searches. When they locate a product, the content delivery service allows users to retrieve it.
- **Content delivery** allows users to replicate files and directories; publish and subscribe to information based on their roles and responsibilities. Content delivery provides timely, assured information transport, including notification when another user reads the information. Multiple, varied communications systems deliver information with delivery and read receipt notifications to provide assured information delivery.
- **Content storage** provides physical and virtual data storage locations on the network with varying degrees of persistence. These information storage capabilities reside throughout the DODIN.

FUNCTIONAL SERVICES

A-166. Information dissemination management and content staging's functional services relate to voice, video, data, and imagery. The enterprise network service effort and the network-enabled enterprise services program deliver these services. These functional services are—

- **Messaging** enables networked information exchange among users and systems. Messaging examples include e-mail, DOD-unique message formats, message-oriented middleware, instant messaging, and alerts.
- **Discovery** helps users discover content or services by exploiting unique descriptions stored in directories, registries, and catalogs. A search engine is an example of a discovery service.
- **Mediation** enables system interoperability by processing data to translate, combine, fuse, or integrate it with other data.
- **Collaboration** allows users to work together with selected capabilities. Chat, online meetings, and workgroup applications are examples of collaboration services.
- **Storage** provides physical and virtual data hosting with varying degrees of persistence, such as archiving, continuity of operations, and content staging. Unit standard operating procedures or operation orders may specify data storage locations.
- **User assistance** provides centralized service desk assistance and automated access to lessons and best practices, which may improve processes or reduce the effort required to perform tasks.

Critical Capabilities

A-167. Content management provides six critical capabilities associated with its functional services. These capabilities are vital at the strategic, operational, and tactical levels across all warfighting functions:

- **Collection of information** is acquiring data based on information requirements.
- **Processing of information** is translating data from one form to another.
- **Storage of information** is recording information to any storage medium on the network.
- **Transmission of information** is conveying information from one place to another, based on prescribed information flow.
- **Display of information** is visually presenting collected information, data, or knowledge.
- **Dissemination of information** uses automation to ensure timely collection, processing, and transmission of information to the right users.

Enabled Effects

A-168. Content management enables information delivery by—

- Retrieving critical information that directly contributes to situational understanding, collaboration, and decision making from systems within the DODIN.
- Compiling retrieved information for processing and storage until needed.
- Caching compiled information in secure systems, according to applicable regulations and policies.
- Cataloging cached information to facilitate future search and discovery.
- Distributing critical information to develop situational understanding, collaborate, or execute decisions.

Information Dissemination Management Principles

A-169. Information dissemination management delivers relevant information from one person or place to another, in a usable form, by any means to improve understanding. Information dissemination management activities use a judicious combination of broadcast and point-to-point dissemination.

Broadcast Dissemination

A-170. Broadcast dissemination allows sending information simultaneously to many users. Anyone who can access the network can receive the information. The greatest advantage of this method is the ability for information managers to reach the widest audience in the shortest time. Since many users with varying information requirements receive it, broadcast dissemination does not tailor the information to a specific commander's needs. Overusing broadcast dissemination can quickly lead to information overload, making it more difficult to find and extract only the relevant information.

Point-to-Point Dissemination

A-171. Point-to-point dissemination directs information to a specific user or set of users. One commander can easily pass information to the next. Information dissemination management personnel tailor information delivery to meet specific requirements, using built-in control mechanisms not present in broadcast dissemination. Each level of command can filter and integrate information, and change it to meet the needs of the next level of command before passing it on. The major disadvantage of point-to-point dissemination is that information reaches a broad audience slowly, with a greater chance of distortion as it passes through the levels of command.

Information Dissemination Management—Scalability

A-172. Information dissemination management allows commanders to configure networks and information systems to meet their information needs. Networks expand or contract to meet the commander's critical information requirements. Scalable network links allow throughput to increase or decrease for specific users. Information dissemination management personnel can set policies so commanders and staff elements receive only specific information and information products. They can also establish separate networks to pass only the information critical to a particular set of users. Ultimately, information dissemination management allows commanders to specify who receives what information, as well as where and when.

NETWORK SITUATIONAL UNDERSTANDING

A-173. Commanders assess the situation and environment through information from staff elements, personal experience, reporting, other sources of information, and the network situational awareness view. Once information is collected, commanders develop their initial understanding by putting it into context.

A-174. DODIN operations allow commanders to receive, correlate, and display an appropriate view of systems and networks to enable near real-time assessment of impacts to current operations. Observing the intensity of network activity, traffic load, and throughput potential yields network situational understanding to enable dynamic rerouting of priority traffic and services, based on system status and capacity. Commanders use the network situational awareness view to—

- Monitor, protect, and prioritize their networks.
- Assess operational impact of network disruptions.
- Respond to network outages or attacks.
- Dynamically reallocate network traffic.

A-175. Each NOSC configures, maintains, and operates network management and intrusion detection software to depict a near real-time view of their network. The NOSC provides this view to the next echelon NOSC so commanders can maintain situational understanding of any network within their area of operations.

This page intentionally left blank.

Glossary

The glossary lists acronyms and terms with Army or joint definitions. Where Army and joint definitions differ, (Army) precedes the definition. Terms for which ATP 6-02.71 is the proponent are marked with an asterisk (*). The proponent publication for other terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

ACOIC	Army Cyber Operations and Integration Center
AOR	area of responsibility
ARCYBER	United States Army Cyber Command
ARFOR	Army forces
BCT	brigade combat team
CJTF	commander, joint task force
COMSEC	communications security
DISN	Defense Information Systems Network
DODIN	Department of Defense information network
***DODIN-A**	Department of Defense information network-Army
ESB	expeditionary signal battalion
G-6	(Army) assistant chief of staff, signal
GCC	geographic combatant commander
IA	information assurance
IAVM	information assurance vulnerability management
INFOCON	information operations condition
IP	Internet protocol
IT	information technology
J-6	communications system directorate of a joint staff
JCC	joint cyberspace center
***NEC**	network enterprise center
NETCOM	United States Army Network Enterprise Technology Command
NIPRNET	Non-classified Internet Protocol Router Network
NOSC	network operations and security center
OPCON	operational control
RCC	regional cyber center
S-6	battalion or brigade signal staff officer
SC(T)	signal command (theater)
SIPRNET	SECRET Internet Protocol Router Network
TNCC	theater network operations control center
USCYBERCOM	United States Cyber Command

WAN	wide-area network
WIN-T	Warfighter Information Network-Tactical

SECTION II – TERMS

configuration management

A discipline applying technical and administrative direction and surveillance to: (1) identify and document the functional and physical characteristics of a configuration item; (2) control changes to those characteristics; and (3) record and report changes to processing and implementation status. (JP 6-0)

critical infrastructure protection

Actions taken to prevent, remediate, or mitigate the man-made or natural risks to critical infrastructure and key assets.. (JP 3-28)

cross domain solution

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

cyber incident

Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein. (CNSSI 4009)

cybersecurity

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

cyberspace defense

Actions normally created within Department of Defense cyberspace for securing, operating, and defending the Department of Defense information network. Specific actions include protect, detect, characterize, counter, and mitigate. (DODI 8500.01)

cyberspace electromagnetic activities

The process of planning, integrating, and synchronizing cyberspace and electronic warfare operations in support of unified land operations. (ADRP 3-0)

defense-in-depth

An information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. (CNSSI 4009)

defensive cyberspace operations-internal defensive measures

Operations in which authorized defense actions occur within the defended portion of cyberspace. (JP 3-12)

defensive cyberspace operations-response actions

Operations that are part of a defensive cyberspace operations mission that are taken external to the defended network or portion of cyberspace without the permission of the owner of the affected system. (JP 3-12)

Department of Defense information network

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

***Department of Defense information network-Army**

An Army-operated enclave of the Department of Defense information network that encompasses all Army information capabilities that collect, process, store, display, disseminate, and protect information worldwide**.** Also called **DODIN-A**.

Department of Defense information network operations

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

electronic attack

Division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. (JP 3-13.1)

electronic protection

Division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. (JP 3-13.1)

enclave

A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter. (CNSSI 4009)

event

Any observable occurrence in a network or system. (CNSSI 4009)

information advantage

The superior position or condition derived from the ability to securely access, share, and collaborate securely via trusted information while exploiting or denying an adversary's ability to do the same. (DODD 8000.01)

information assurance vulnerability management

The comprehensive distribution process for notifying combatant commands, Services. Department of Defense agencies, and Department of Defense field activities about vulnerability alerts, bulletins, technical advisories, and countermeasures information. The information assurance vulnerability management program requires combatant commands, Services, Department of Defense agencies, and Department of Defense field activities receipt acknowledgment and provides specific time parameters for implementing appropriate countermeasures depending on the criticality of the vulnerability. Also called **IAVM.** (CJCSM 6510.01)

information environment

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

information security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. (CNSSI 4009)

insider threat

The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities. (CNSSI 4009)

local area network

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

***network enterprise center**

The facility that provides and acquires telecommunications and information management services on Army installations. Also called **NEC.**

operations security

A capability that identifies and controls critical information, indicators of friendly force actions attendant to military operations, and incorporates countermeasures to reduce the risk of an adversary exploiting vulnerabilities. (JP 3-13.3)

platform information technology

Information technology, both hardware and software, that is physically part of, dedicated to, or essential in real-time to the mission performance of special purpose systems. (DODI 8500.01)

reachback

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

regional hub node

A component of the network service center, which provides a transport connection between the Warfighter Information Network-Tactical and the wider Department of Defense information network. (ATP 6-02.60)

remediation

The act of mitigating a vulnerability or a threat. (CNSSI 4009)

spectrum management operations

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

spillage

A security incident that results in the transfer of classified information onto an information system not authorized to store or process that information. (CNSSI 4009)

sustainment warfighting function

The related tasks and systems that provide support and services to ensure freedom of action, extend operational reach, and prolong endurance. (ADP 3-0)

***technical channels**

(Army) The chain of authority for ensuring the execution of clearly delineated technical tasks, functions, and capabilities to meet the dynamic requirements of Department of Defense information network operations.

wide-area network

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

This page intentionally left blank.

References

All URLs accessed on 29 March 2019.

REQUIRED PUBLICATIONS

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

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

DOD Dictionary of Military and Associated Terms. February 2019.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS

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

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

CJCSM 6510.03. *Department of Defense Cyber Red Team Certification and Accreditation*. 28 February 2013.

DODD 5400.07. *DOD Freedom of Information Act (FOIA) Program*. 5 April 2019.

DODD 8000.01. *Management of the Department of Defense Information Enterprise*. 17 March 2016.

DODD 8115.01. *Information Technology Portfolio Management*. 10 October 2005.

DODD 8140.01. *Cybersecurity Workforce Management.* 11 August 2015.

DODI 5240.26. *Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat*. 4 May 2012.

DODI 8410.02. *NetOps for the Global Information Grid*. 19 December 2008.

DODI 8410.03. *Network Management*. 29 August 2012.

DODI 8500.01. *Cybersecurity*. 14 March 2014.

DODI 8510.01. *Risk Management Framework (RMF) for DOD Information Technology (IT)*. 12 March 2014.

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

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

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

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

JP 3-13.3. *Operations Security*. 6 January 2016.

JP 3-28. *Defense Support of Civil Authorities*. 29 October 2018.

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

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

JP 5-0. *Joint Planning*. 16 June 2017.

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

ARMY PUBLICATIONS

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

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

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

ADP 4-0. *Sustainment*. 31 July 2012.

ADP 5-0. *The Operations Process*. 17 May 2012.

ADRP 3-0, *Operations*. 6 October 2017.

ADRP 5-0. *The Operations Process*. 17 May 2012.

AR 25-1. *Army Information Technology*. 25 June 2013.

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

AR 380-53. *Communications Security Monitoring*. 23 December 2011.

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

AR 500-3. *U.S. Army Continuity of Operations Program Policy and Planning*. 18 April 2008.

ATP 3-05.60. *Special Operations Communications System*. 30 November 2015.

ATP 3-36. *Electronic Warfare Techniques*. 16 December 2014.

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

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

ATP 6-02.60. *Techniques for Warfighter Information Network-Tactical*. 3 February 2016.

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

ATP 6-02.75. *Techniques for Communications Security (COMSEC) Operations*. 17 August 2015.

DA Pam 25-1-2. *Information Technology Contingency Planning*. 6 June 2012.

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

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

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

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

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

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

OTHER PUBLICATIONS

American National Standard T1.523.2011. Alliance for Telecommunications Industry Solutions Telecom Glossary 2011. https://glossary.atis.org/.

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

Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*. February 2004. https://csrc.nist.gov/publications/detail/fips/199/final.

National Institute of Standards and Technology Special Publication 800-30 Rev.1. *Guide for Conducting Risk Assessments*. 17 September 2012. https://csrc.nist.gov/publications/sp.

National Institute of Standards and Technology Special Publication 800-53 Rev. 5. *Security and Privacy Controls for Information Systems and Organizations*. 15 August 2017. https://csrc.nist.gov/publications/sp.

Strategic Instruction 527-1. Department of Defense (DOD) Information Operations Condition (INFOCON) System Procedures. 27 March 2015. https://powhatan.iiie.disa.mil/policy-guidance/d527-01.pdf. (Requires DOD-approved certificate login)

RECOMMENDED READINGS

ADRP 1. *The Army Profession*. 14 June 2015.

ADRP 6-0. *Mission Command*. 17 May 2012.

CJCSI 6510.01F. *Information Assurance (IA) and Support to Computer Network Defense (CND)*. 9 February 2011.

DODI 8530.01. *Cybersecurity Activities Support to DOD Information Network Operations*. 7 March 2016.

WEBSITES

These are the websites quoted or paraphrased in this publication.

Army Cybersecurity Portal https://www.milsuite.mil/wiki/Portal:Army_Cybersecurity. (Requires DOD-approved certificate login)

Defense Enterprise Portal Service https://www.disa.mil/Services/Enterprise-Services/Applications/DoD-Enterprise-Portal. (Requires DOD-approved certificate login)

Information Assurance Support Environment https://iase.disa.mil/stigs/Pages/index.aspx. (Requires DOD-approved certificate login)

National Institute of Standards and Technology Computer Security Resource Center (Special Publications Library) https://csrc.nist.gov/publications/sp.

National Institute of Standards and Technology Cybersecurity Framework https://www.nist.gov/cyberframework/index.cfm.

National Vulnerability Database https://nvd.nist.gov.

Open Vulnerability and Assessment Language Repository https://oval.cisecurity.org/repository.

PRESCRIBED FORMS

None.

REFERENCED FORMS

Unless otherwise indicated, Department of the Army forms are available on the Army Publishing Directorate website: https://armypubs.army.mil.

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

This page intentionally left blank.

Index

Entries are by paragraph number unless indicated otherwise.

ATP 6-02.71
30 April 2019

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

Kathleen S. Miller

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army
1911505

DISTRIBUTION:
Distributed in electronic media only(EMO).